#3

P20745.P04

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant :M. AKIMOTO et al.

Serial No. :Not Yet Assigned

Filed :Concurrently Herewith

For :A COMMUNICATION CONTROL APPARATUS AND A COMMUNICATION CONTROL METHOD

CLAIM OF PRIORITY

Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Applicant hereby claims the right of priority granted pursuant to 35 U.S.C. 119 based upon Japanese Application No. 2000-236917, filed August 4, 2000. As required by 37 C.F.R. 1.55, a certified copy of the Japanese application is being submitted herewith.

Respectfully submitted,
M. AKIMOTO et al.

Leslie J. Paperner Reg No. 33,329
Bruce H. Bernstein
Reg. No. 29,027

August 2, 2001
GREENBLUM & BERNSTEIN, P.L.C.
1941 Roland Clarke Place
Reston, VA 20191
(703) 716-1191

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ８月 ４日

出 願 番 号
Application Number: 特願２０００－２３６９１７

出 願 人
Applicant (s): 松下電送システム株式会社

２００１年 ３月 ２日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２００１－３０１５３８４

【書類名】　特許願
【整理番号】　2952020019
【提出日】　平成12年 8月 4日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/00
【発明者】
　【住所又は居所】　東京都目黒区下目黒２丁目３番８号　松下電送システム株式会社内
　【氏名】　秋元　正男
【発明者】
　【住所又は居所】　東京都目黒区下目黒２丁目３番８号　松下電送システム株式会社内
　【氏名】　村田　松寿
【特許出願人】
　【識別番号】　000187736
　【氏名又は名称】　松下電送システム株式会社
【代理人】
　【識別番号】　100105050
　【弁理士】
　【氏名又は名称】　鷲田　公一
【手数料の表示】
　【予納台帳番号】　041243
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9603473
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　通信制御装置及び通信制御方法

【特許請求の範囲】

【請求項１】　インターネットファクシミリ装置に接続される第１インタフェース部と、前記インターネットファクシミリ装置が接続され、サーバ装置によりＨＴＴＰプロトコルで管理されるネットワークに接続される第２インタフェース部と、前記インターネットファクシミリ装置との間でＳＭＴＰプロトコルに従って通信を制御するＳＭＴＰ処理部と、前記サーバ装置との間でＨＴＴＰプロトコルに従って通信を制御するＨＴＴＰ処理部と、前記インターネットファクシミリ装置から電子メールデータを受信する電子メール通信部と、前記電子メールデータをＨＴＭＬデータに変換するＨＴＭＬ処理部と、前記ＨＴＭＬデータを前記サーバ装置に送信するＨＴＭＬ通信部と、を具備することを特徴とする通信制御装置。

【請求項２】　前記第１インタフェース部を介して送信される信号種別を判定する信号種別判定部を具備し、前記信号種別判定部が前記インターネットファクシミリ装置から所定の信号種別を判定した場合、前記ＨＴＴＰ処理部は、前記サーバ装置との間でＨＴＴＰプロトコルに従って通信の制御を開始する一方、前記ＳＭＴＰ処理部は、前記インターネットファクシミリ装置との間でＳＭＴＰプロトコルに従って通信を制御することを特徴とする請求項１記載の通信制御装置。

【請求項３】　前記ＨＴＴＰ処理部は、前記信号種別判定部が前記インターネットファクシミリ装置からＳＭＴＰプロトコルに従ったコマンド信号である「ＨＥＬＯ」を受信した場合に前記サーバ装置との間でＨＴＴＰプロトコルに従って通信の制御を開始することを特徴とする請求項２記載の通信制御装置。

【請求項４】　前記電子メール通信部が受信した電子メールデータに対して暗号化処理を行う暗号化処理部を具備し、前記ＨＴＭＬ処理部は、前記暗号化処理部が暗号化処理を施した電子メールデータをＨＴＭＬデータに変換することを特徴とする請求項１から請求項３のいずれかに記載の通信制御装置。

【請求項５】　前記暗号化処理部の暗号化処理に必要となる情報を格納する

ＩＣカードと、前記ＩＣカードが挿入されるスロット部と、を具備し、前記暗号化処理部は、前記スロット部に前記ＩＣカードが挿入されている場合に当該ＩＣカード内の前記情報を用いて暗号化処理を行うことを特徴とする請求項４記載の通信制御装置。

【請求項６】　インターネットファクシミリ装置に接続される第１インタフェース部と、前記インターネットファクシミリ装置が接続され、サーバ装置によりＨＴＴＰプロトコルで管理されるネットワークに接続される第２インタフェース部と、前記インターネットファクシミリ装置との間でＰＯＰ３プロトコルに従って通信を制御するＰＯＰ３処理部と、前記サーバ装置との間でＨＴＴＰプロトコルに従って通信を制御するＨＴＴＰ処理部と、前記サーバ装置から電子メールデータを含むＨＴＭＬデータを受信するＨＴＭＬ通信部と、前記ＨＴＭＬデータから電子メールデータを取り出すＨＴＭＬ処理部と、前記インターネットファクシミリ装置に前記電子メールデータを送信する電子メール通信部と、を具備することを特徴とする通信制御装置。

【請求項７】　前記第１インタフェース部を介して送信される信号種別を判定する信号種別判定部を具備し、前記信号種別判定部が前記インターネットファクシミリ装置から所定の信号種別を判定した場合、前記ＨＴＴＰ処理部は、前記サーバ装置との間でＨＴＴＰプロトコルに従って通信の制御を開始する一方、前記ＰＯＰ３処理部は、前記インターネットファクシミリ装置との間でＰＯＰ３プロトコルに従って通信を制御することを特徴とする請求項６記載の通信制御装置。

【請求項８】　前記ＨＴＴＰ処理部は、前記信号種別判定部が前記インターネットファクシミリ装置からＰＯＰ３プロトコルに従ったコマンド信号である「ＵＳＥＲ」を受信した場合に前記サーバ装置との間でＨＴＴＰプロトコルに従って通信の制御を開始することを特徴とする請求項７記載の通信制御装置。

【請求項９】　前記ＨＴＭＬ処理部がＨＴＭＬデータから取り出した電子メールデータに暗号化処理が施されている場合に復号化処理を行う復号化処理部を具備し、前記電子メール通信部は、前記復号化処理部が復号化処理を行った電子メールデータを前記インターネットファクシミリ装置に送信することを特徴とす

る請求項６から請求項８のいずれかに記載の通信制御装置。

【請求項１０】　前記復号化処理部の復号化処理に必要となる情報を格納するＩＣカードと、前記ＩＣカードが挿入されるスロット部と、を具備し、前記復号化処理部は、前記スロット部に前記ＩＣカードが挿入されている場合に当該ＩＣカード内の前記情報を用いて復号化処理を行うことを特徴とする請求項９記載の通信制御装置。

【請求項１１】　前記ＩＣカードは、電子メールアドレス情報を格納し、前記ＨＴＭＬ通信部は、前記スロット部に前記ＩＣカードが挿入されている場合に当該ＩＣカード内の前記電子メールアドレス情報に着信した電子メールデータに対応するＨＴＭＬデータを受信することを特徴とする請求項１０記載の通信制御装置。

【請求項１２】　インターネットファクシミリ装置に接続される第１インタフェース部からＳＭＴＰプロトコルに従った所定の信号種別を判定する工程と、前記所定の信号種別を判定した場合に前記インターネットファクシミリ装置との間でＳＭＴＰプロトコルに従って通信を制御する一方、前記インターネットファクシミリ装置が接続され、サーバ装置によりＨＴＴＰプロトコルで管理されるネットワークに接続される第２インタフェース部を介して前記サーバ装置との間でＨＴＴＰプロトコルに従って通信を制御する工程と、前記インターネットファクシミリ装置から電子メールデータを受信する工程と、前記電子メールデータをＨＴＭＬデータに変換する工程と、前記ＨＴＭＬデータを前記サーバ装置に送信する工程と、を具備することを特徴とする通信制御方法。

【請求項１３】　インターネットファクシミリ装置に接続される第１インタフェース部からＰＯＰ３プロトコルに従った所定の信号種別を判定する工程と、前記所定の信号種別を判定した場合に前記インターネットファクシミリ装置との間でＰＯＰ３プロトコルに従って通信を制御する一方、前記インターネットファクシミリ装置が接続され、サーバ装置によりＨＴＴＰプロトコルで管理されるネットワークに接続される第２インタフェース部を介して前記サーバ装置との間でＨＴＴＰプロトコルに従って通信を制御する工程と、前記サーバ装置から電子メールデータを含むＨＴＭＬデータを受信する工程と、前記ＨＴＭＬデータから電

子メールデータを取り出す工程と、取り出した前記電子メールデータを前記インターネットファクシミリ装置に送信する工程と、を具備することを特徴とする通信制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、インターネットファクシミリ装置とネットワークとの間に接続され、双方の間で通信制御を行う通信制御装置及び通信制御方法に関する。

【０００２】

【従来の技術】

従来、企業などの組織内の情報共有を効率的に行うためにグループウェアソフトを利用してネットワークを構築することが行われている。近年、このようなネットワーク（以下、「グループウェアネットワーク」という）には、インターネット技術を取り入れ、ＷＷＷブラウザから利用可能なグループウェアソフトが採用されることが多い。この場合、そのグループウェアネットワーク上のＰＣ等のクライアント端末は、ＷＷＷブラウザを利用することで、グループウェアネットワーク上で情報を共有することができる。これにより、クライアント端末は、電子メールや電子掲示板等の機能を実現することができる。

【０００３】

一方、近年、一般的なファクシミリと同様の操作で画情報をインターネット経由で送信するファクシミリ装置が開発されている。この種のファクシミリは、通信経路の全部又は一部にインターネットを使用することからインターネットファクシミリ装置（以下、「ＩＦＡＸ」という）と呼ばれている。このようなＩＦＡＸは、画情報の送信時は、ファクシミリデータを電子メールのフォーマットに変換して送信する。一方、画情報の受信時は、受信した電子メールデータをファクシミリのフォーマットに変換して印刷処理を行う。このとき、ＩＦＡＸは、電子メールデータの通信をＳＭＴＰ（Simple Mail Transfer Protocol）やＰＯＰ３（Post Office Protocol Version3）等のプロトコルに従って制御している。

【０００４】

【発明が解決しようとする課題】

しかしながら、上述のようなWWWブラウザを利用したグループウェアネットワークにおいては、各種データは、ＨＴＴＰプロトコルに従って通信が行われる。このため、ＳＭＴＰ（Simple Mail Transfer Protocol）やＰＯＰ３（Post Office Protocol Version3）に従って通信を制御するＩＦＡＸは、動作することができないという問題がある。

【０００５】

本発明は、かかる点に鑑みてなされたものであり、ＨＴＴＰプロトコルで管理されたネットワーク上でもＩＦＡＸを正常に動作させることができる通信制御装置及び通信制御方法を提供することを目的とする。

【０００６】

【課題を解決するための手段】

本発明は、ＩＦＡＸに接続される第１インタフェース部からＳＭＴＰプロトコルに従った所定の信号種別を判定し、所定の信号種別を判定した場合にＩＦＡＸとの間でＳＭＴＰプロトコルに従って通信を制御する一方、ＩＦＡＸが接続され、サーバ装置によりＨＴＴＰプロトコルで管理されるネットワークに接続される第２インタフェース部を介して、サーバ装置との間でＨＴＴＰプロトコルに従って通信を制御しながら、ＩＦＡＸから電子メールデータを受信し、受信した電子メールデータをＨＴＭＬデータに変換し、さらにそのＨＴＭＬデータをサーバ装置に送信するようにしたものである。

【０００７】

これにより、ＩＦＡＸからサーバ装置に電子メールを送信する際、ＩＦＡＸとの間でＳＭＴＰに従って各種信号や電子メールデータの通信を行う一方、サーバ装置との間でＨＴＴＰプロトコルに従って各種信号や電子メールデータの通信を行う。このため、ＨＴＴＰプロトコルで管理されるネットワークにおいても、ＩＦＡＸは、正常に電子メールの送信動作を行うことができる。

【０００８】

また、本発明は、ＩＦＡＸに接続される第１インタフェース部からＰＯＰ３プロトコルに従った所定の信号種別を判定し、所定の信号種別を判定した場合にＩ

ＦＡＸとの間でＰＯＰ３プロトコルに従って通信を制御する一方、ＩＦＡＸが接続され、サーバ装置によりＨＴＴＰプロトコルで管理されるネットワークに接続される第２インタフェース部を介して、サーバ装置との間でＨＴＴＰプロトコルに従って通信を制御しながら、サーバ装置から電子メールデータを含むＨＴＭＬデータを受信し、受信したＨＴＭＬデータから電子メールデータを取り出し、取り出した電子メールデータをＩＦＡＸに送信するようにしたものである。

【０００９】

これにより、ＩＦＡＸがサーバ装置から電子メールを受信する際、ＩＦＡＸとの間でＰＯＰ３プロトコルに従って各種信号や電子メールデータの通信を行う一方、サーバ装置との間でＨＴＴＰプロトコルに従って各種信号や電子メールデータの通信を行う。このため、ＨＴＴＰプロトコルで管理されたネットワークにおいても、ＩＦＡＸは、正常に電子メールの受信動作を行うことができる。

【００１０】

【発明の実施の形態】

本発明の第１の態様に係る通信制御装置は、インターネットファクシミリ装置に接続される第１インタフェース部と、前記インターネットファクシミリ装置が接続され、サーバ装置によりＨＴＴＰプロトコルで管理されるネットワークに接続される第２インタフェース部と、前記インターネットファクシミリ装置との間でＳＭＴＰプロトコルに従って通信を制御するＳＭＴＰ処理部と、前記サーバ装置との間でＨＴＴＰプロトコルに従って通信を制御するＨＴＴＰ処理部と、前記インターネットファクシミリ装置から電子メールデータを受信する電子メール通信部と、前記電子メールデータをＨＴＭＬデータに変換するＨＴＭＬ処理部と、前記ＨＴＭＬデータを前記サーバ装置に送信するＨＴＭＬ通信部と、を具備する構成を採る。

【００１１】

この構成によれば、ＩＦＡＸからサーバ装置に電子メールを送信する際、ＩＦＡＸとの間でＳＭＴＰプロトコルに従って各種信号や電子メールデータの通信を行う一方、サーバ装置との間でＨＴＴＰプロトコルに従って各種信号や電子メールデータの通信を行う。このため、ＨＴＴＰプロトコルで管理されるネットワー

クにおいても、ＩＦＡＸは、正常に電子メールの送信動作を行うことができる。

【００１２】

本発明の第２の態様に係る通信制御装置は、第１の態様において、前記第１インタフェース部を介して送信される信号種別を判定する信号種別判定部を具備し、前記信号種別判定部が前記インターネットファクシミリ装置から所定の信号種別を判定した場合、前記ＨＴＴＰ処理部は、前記サーバ装置との間でＨＴＴＰプロトコルに従って通信の制御を開始する一方、前記ＳＭＴＰ処理部は、前記インターネットファクシミリ装置との間でＳＭＴＰプロトコルに従って通信を制御する構成を採る。

【００１３】

本発明の第３の態様に係る通信制御装置は、第２の態様において、前記ＨＴＴＰ処理部は、前記信号種別判定部が前記インターネットファクシミリ装置からＳＭＴＰプロトコルに従ったコマンド信号である「ＨＥＬＯ」を受信した場合に前記サーバ装置との間でＨＴＴＰプロトコルに従って通信の制御を開始する構成を採る。

【００１４】

これらの構成によれば、インターネットファクシミリ装置から所定の信号（第３の態様では、「ＨＥＬＯ」）を受信した場合に、ＨＴＴＰ処理部がサーバ装置とＨＴＴＰプロトコルに従って通信制御を行う。これと並行して、ＳＭＴＰ処理部がインターネットファクシミリ装置とＳＭＴＰプロトコルに従って通信制御を行う。このため、インターネットファクシミリ装置とサーバ装置との間において、リアルタイムで通信制御を行うことができる。これにより、いずれか一方との通信を完了した後に他方と通信を開始するような場合に発生する事態を防止することができる。例えば、送信済みデータを削除することによって、同一データの再送ができないような事態が防止される。なお、ここでは、第３の態様で「ＨＥＬＯ」を具体例として説明しているが、これ以外のＳＭＴＰプロトコルに従ったコマンド信号（例えば、「ＭＡＩＬ」、「ＲＣＰＴ」等）であってもよい。

【００１５】

本発明の第４の態様に係る通信制御装置は、第１から第３のいずれかの態様に

おいて、前記電子メール通信部が受信した電子メールデータに対して暗号化処理を行う暗号化処理部を具備し、前記ＨＴＭＬ処理部は、前記暗号化処理部が暗号化処理を施した電子メールデータをＨＴＭＬデータに変換する構成を採る。

【００１６】

この構成によれば、暗号化処理部がその暗号化処理を施した電子メールデータがＨＴＭＬデータに変換されてサーバ装置に送信される。これにより、ＨＴＴＰプロトコルで管理されるネットワークにおいても、ＩＦＡＸは、正常に電子メールの送信動作を行うことができると共に、既存のインターネットファクシミリ装置に特別な構成を附加することなく、インターネットファクシミリ装置から送信される電子メールの秘匿性を確保することができる。

【００１７】

本発明の第５の態様に係る通信制御装置は、第４の態様において、前記暗号化処理部の暗号化処理に必要となる情報を格納するＩＣカードと、前記ＩＣカードが挿入されるスロット部と、を具備し、前記暗号化処理部は、前記スロット部に前記ＩＣカードが挿入されている場合に当該ＩＣカード内の前記情報を用いて暗号化処理を行う構成を採る。

【００１８】

この構成によれば、ＩＣカードがスロット部に挿入されている場合にのみ、その内部に格納された情報に基づいて暗号化処理が施されるため、簡単に暗号化処理の要否を判断することができる。

【００１９】

本発明の第６の態様に係る通信制御装置は、インターネットファクシミリ装置に接続される第１インタフェース部と、前記インターネットファクシミリ装置が接続され、サーバ装置によりＨＴＴＰプロトコルで管理されるネットワークに接続される第２インタフェース部と、前記インターネットファクシミリ装置との間でＰＯＰ３プロトコルに従って通信を制御するＰＯＰ３処理部と、前記サーバ装置との間でＨＴＴＰプロトコルに従って通信を制御するＨＴＴＰ処理部と、前記サーバ装置から電子メールデータを含むＨＴＭＬデータを受信するＨＴＭＬ通信部と、前記ＨＴＭＬデータから電子メールデータを取り出すＨＴＭＬ処理部と、

前記インターネットファクシミリ装置に前記電子メールデータを送信する電子メール通信部と、を具備する構成を採る。

【００２０】

この構成によれば、ＩＦＡＸがサーバ装置から電子メールを受信する際、ＩＦＡＸとの間でＰＯＰ３プロトコルに従って各種信号や電子メールデータの通信を行う一方、サーバ装置との間でＨＴＴＰプロトコルに従って各種信号や電子メールデータの通信を行う。このため、ＨＴＴＰプロトコルで管理されたネットワークにおいても、ＩＦＡＸは、正常に電子メールの受信動作を行うことができる。

【００２１】

本発明の第７の態様に係る通信制御装置は、第６の態様において、前記第１インタフェース部を介して送信される信号種別を判定する信号種別判定部を具備し、前記信号種別判定部が前記インターネットファクシミリ装置から所定の信号種別を判定した場合、前記ＨＴＴＰ処理部は、前記サーバ装置との間でＨＴＴＰプロトコルに従って通信の制御を開始する一方、前記ＰＯＰ３処理部は、前記インターネットファクシミリ装置との間でＰＯＰ３プロトコルに従って通信を制御する構成を採る。

【００２２】

本発明の第８の態様に係る通信制御装置は、第７に態様において、前記ＨＴＴＰ処理部は、前記信号種別判定部が前記インターネットファクシミリ装置からＰＯＰ３プロトコルに従ったコマンド信号である「ＵＳＥＲ」を受信した場合に前記サーバ装置との間でＨＴＴＰプロトコルに従って通信の制御を開始する構成を採る。

【００２３】

これらの構成によれば、インターネットファクシミリ装置から所定の信号（第８の態様では、「ＵＳＥＲ」）を受信した場合に、ＨＴＴＰ処理部がサーバ装置とＨＴＴＰプロトコルに従って通信制御を行う。これと並行して、ＰＯＰ３処理部がインターネットファクシミリ装置とＰＯＰプロトコルに従って通信制御を行う。このため、インターネットファクシミリ装置とサーバ装置との間において、リアルタイムで通信制御を行うことができる。これにより、いずれか一方との通

信を完了した後に他方と通信を開始するような場合に発生する事態を防止することができる。

【００２４】

本発明の第９の態様に係る通信制御装置は、第６から第８のいずれかの態様において、前記ＨＴＭＬ処理部がＨＴＭＬデータから取り出した電子メールデータに暗号化処理が施されている場合に復号化処理を行う復号化処理部を具備し、前記電子メール通信部は、前記復号化処理部が復号化処理を行った電子メールデータを前記インターネットファクシミリ装置に送信する構成を採る。

【００２５】

この構成によれば、ＨＴＭＬデータから取り出した電子メールデータに暗号化処理が施されている場合、復号化処理が行われた電子メールデータがインターネットファクシミリ装置に送信される。これにより、ＨＴＴＰプロトコルで管理されたネットワークにおいても、ＩＦＡＸは、正常に電子メールの受信動作を行うことができると共に、既存のインターネットファクシミリ装置に特別な構成を附加することなく、インターネットファクシミリ装置から送信される電子メールの秘匿性を確保することができる。

【００２６】

本発明の第１０の態様に係る通信制御装置は、第９の態様において、前記復号化処理部の復号化処理に必要となる情報を格納するＩＣカードと、前記ＩＣカードが挿入されるスロット部と、を具備し、前記復号化処理部は、前記スロット部に前記ＩＣカードが挿入されている場合に当該ＩＣカード内の前記情報を用いて復号化処理を行う構成を採る。

【００２７】

この構成によれば、ＩＣカードがスロット部に挿入されている場合にのみ、その内部に格納された情報に基づいて復号化処理が施されるため、簡単に復号化処理の要否を判断することができる。

【００２８】

本発明の第１１の態様に係る通信制御装置は、第１０の態様において、前記ＩＣカードは、電子メールアドレス情報を格納し、前記ＨＴＭＬ通信部は、前記ス

ロット部に前記ＩＣカードが挿入されている場合に当該ＩＣカード内の前記電子メールアドレス情報に着信した電子メールデータに対応するＨＴＭＬデータを受信する構成を採る。

【００２９】

この構成によれば、電子メール通信部は、ＩＣカードがスロット部に挿入されている場合にのみ電子メールデータの受信処理を行う。このとき、電子メールデータの受信処理は、そのＩＣカード内に格納された電子メールアドレス情報を用いて行われる。このため、接続されたインターネットファクシミリ装置を多人数で使用する場合においても、自分のメールアドレスに届いた電子メールデータを他人に見られることなく受信することができる。これにより、他人に自分宛ての電子メールデータを見られるという事態を防止することができ、より電子メールデータの秘匿性を確保することができる。

【００３０】

本発明の第１２の態様に係る通信制御方法は、インターネットファクシミリ装置に接続される第１インタフェース部からＳＭＴＰプロトコルに従った所定の信号種別を判定する工程と、前記所定の信号種別を判定した場合に前記インターネットファクシミリ装置との間でＳＭＴＰプロトコルに従って通信を制御する一方、前記インターネットファクシミリ装置が接続され、サーバ装置によりＨＴＴＰプロトコルで管理されるネットワークに接続される第２インタフェース部を介して前記サーバ装置との間でＨＴＴＰプロトコルに従って通信を制御する工程と、前記インターネットファクシミリ装置から電子メールデータを受信する工程と、前記電子メールデータをＨＴＭＬデータに変換する工程と、前記ＨＴＭＬデータを前記サーバ装置に送信する工程と、を具備するようにしたものである。

【００３１】

本発明の第１３の態様に係る通信制御方法は、インターネットファクシミリ装置に接続される第１インタフェース部からＰＯＰ３プロトコルに従った所定の信号種別を判定する工程と、前記所定の信号種別を判定した場合に前記インターネットファクシミリ装置との間でＰＯＰ３プロトコルに従って通信を制御する一方、前記インターネットファクシミリ装置が接続され、サーバ装置によりＨＴＴＰ

プロトコルで管理されるネットワークに接続される第２インタフェース部を介して前記サーバ装置との間でＨＴＴＰプロトコルに従って通信を制御する工程と、前記サーバ装置から電子メールデータを含むＨＴＭＬデータを受信する工程と、前記ＨＴＭＬデータから電子メールデータを取り出す工程と、取り出した前記電子メールデータを前記インターネットファクシミリ装置に送信する工程と、を具備するようにしたものである。

【００３２】

以下、本発明の実施の形態について図面を参照して詳細に説明する。

【００３３】

（実施の形態１）

図１は、本発明の実施の形態１に係る通信制御装置が動作するネットワークを示す概念図である。本実施の形態の通信制御装置１００は、ＩＦＡＸ１０１に接続され、ＩＦＡＸ１０１とそれに接続されたネットワークとの間で電子メール通信を行う場合に、その通信プロトコルを変換するアダプタとして機能するため、本実施の形態においては、以下、単にアダプタ（ＡＤＰＴ）と呼ぶこととする。

【００３４】

このようなＩＦＡＸ１０１に接続されたＡＤＰＴ１００は、ＰＣ等の通信端末１０２と共に、ＬＡＮ（Local Area Network）等のネットワーク１０３に接続されている。このネットワーク１０３は、グループウェアソフトを利用したサーバ（以下、「グループウェアサーバ」という）１０４により管理されている。以下において、このグループウェアサーバ１０４に管理されるネットワーク１０３をグループウェアネットワーク１０３と呼ぶこととする。

【００３５】

このグループウェアサーバ１０４は、例えば、ＬＯＴＵＳ社（米国）のＮＯＴＥＳ等のグループウェアソフトを採用し社内ネットワークを構築する。これにより、ＰＣ１０２等のクライアント端末は、グループウェアネットワーク１０３で情報の共有を実現することができる。また、グループウェアサーバ１０４は、ＷＥＢサーバとしての機能を有し、グループウェアネットワーク１０３に接続されたＰＣ１０２等のクライアント端末、あるいは、外部のクライアント端末は、Ｗ

ＷＷブラウザを利用することでグループウェアネットワーク１０３における情報の共有を実現することができる。本実施の形態に係る発明は、グループウェアサーバ１０４がＷＥＢサーバとして機能する場合に顕著な効果を奏するため、特にこの場合について説明する。

【００３６】

このグループウェアネットワーク１０３の外部にあるＬＡＮ１０５に接続されたＰＣ１０６が電子メールをグループウェアネットワーク１０３上のＰＣ１０２等のクラインアント端末に送信する場合、ＰＣ１０６等から送信された電子メールは、ＬＡＮ１０５を介してメールサーバ１０７に送信される。そして、メールサーバ１０７で送信先等が判断され、インターネット１０８を介してグループウェアサーバ１０４に転送される。

【００３７】

グループウェアサーバ１０４は、外部からの電子メールを受信すると、そのアドレス情報からユーザ名を判断する。そして、ユーザ名に対応するクライアントがグループウェアネットワーク１０３上に存在するか判断し、存在する場合には、そのユーザ名に対応するメールボックスに受信した電子メールデータを格納する。そして、そのユーザ名に対応するクライアント端末からアクセスがあった場合、その受信した電子メールをＷＷＷブラウザ上で表示できるように電子メールデータの変換処理を行う。これにより、ＰＣ１０２等のクライアント端末は、ＷＷＷブラウザ上で電子メールを見ることができる。

【００３８】

図２は、このような場合におけるグループウェアサーバ１０４及びグループウェアネットワーク１０３上のＰＣ１０２等のクライアント端末周辺における通信プロトコルを説明するための概念図である。

【００３９】

ＬＡＮ１０５に接続されたＰＣ１０６からグループウェアネットワーク１０３上のＰＣ１０２に電子メールを送信する場合、インターネット１０８を介して電子メールは、ＳＭＴＰプロトコルに従ってグループウェアサーバ１０４に送信される。この電子メールは、グループウェアサーバ１０４において一時的に保持さ

れる。そして、ＰＣ１０２から要求があった場合にグループウェアサーバ１０４は、その電子メールのプロトコルをＳＭＴＰプロトコルからＨＴＴＰプロトコルに変換することでＰＣ１０２のWWWブラウザ上で見ることができるようにしている。

【００４０】

なお、図２において、ファイアウォール（ＦＩＲＥ　ＷＡＬＬ）は、インターネット１０８とグループウェアネットワーク１０３との間に配設され、インターネット１０８からのデータの流入を防止し、グループウェアネットワーク１０３上のクライアント端末からの要求に応答するデータだけグループウェアネットワーク１０３内に受け入れる機能を有するものである。

【００４１】

これに対して、ＬＡＮ１０５に接続されたＩＦＡＸ１０９が電子メールをグループウェアネットワーク１０３上のＩＦＡＸ１０１に送信する場合、ＰＣ１０６からの電子メールと同様に、ＩＦＡＸ１０９からメールサーバ１０７、インターネット１０８を介してグープウェアサーバ１０４に転送される。そして、グループウェアサーバ１０４でユーザ名が判断され、そのユーザ名に対応するクライアントが存在する場合には、そのユーザ名に対応したメールボックスに受信した電子メールデータが格納される。さらに、そのユーザ名に対応するＩＦＡＸ１０１からＡＤＰＴ１００を介してアクセスがあった場合、ＰＣ１０６からの電子メールと同様に、その受信した電子メールデータの変換処理を行う。

【００４２】

図２を用いて説明すると、ＬＡＮ１０５に接続されたＩＦＡＸ１０９からグループウェアネットワーク１０３上のＩＦＡＸ１０１に電子メールを送信する場合、上述のＰＣ１０６からの電子メールと同様に、インターネット１０８を介して電子メールは、ＳＭＴＰプトロコルに従ってグループウェアサーバ１０４に送信される。この電子メールは、グループウェアサーバ１０４において一時的に保持される。そして、ＩＦＡＸ１０１からＡＤＰＴ１００を介して要求があった場合にグループウェアサーバ１０４は、その電子メールのプロトコルをＳＭＴＰプロトコルからＨＴＴＰプロトコルに変換するようにしている。

【００４３】

ＡＤＰＴ１００は、このＨＴＴＰプロトコルに従って処理された電子メールデータを受け取り、ＩＦＡＸ１０１との間でさらにプロトコルの変換処理を行う。すなわち、ＡＤＰＴ１００は、ＩＦＡＸ１０１の動作可能なプロトコルであるＰＯＰ３（送信時には、ＳＭＴＰ）に従って電子メールデータをＩＦＡＸ１０１に受け渡す。これにより、ＩＦＡＸ１０１は、通常の電子メールの通信処理と同様に、電子メールの受信を行うことができ、受信したその電子メールの印刷を行うことができる。

【００４４】

図３は、上述のような機能を有する本ＡＤＰＴ１００のハードウエア構成を示すブロック図である。

【００４５】

中央処理部（ＣＰＵ）２００は、各種プログラムを実行してＡＤＰＴ１００の各部を制御する。ＲＯＭ２０１は、ＣＰＵ２００が実行するプログラムを格納する。ＲＡＭ２０２は、プログラムのデータ領域として使用されると共に、所定のデータを格納するメモリとして使用される。

【００４６】

第１ＬＡＮインタフェース（以下、「第１ＬＡＮＩ／Ｆ」という）２０３は、グループウェアネットワーク１０３との間のデータの送受信を制御するインタフェースである。第２ＬＡＮインタフェース（以下、「第２ＬＡＮＩ／Ｆ」という）２０４は、ＩＦＡＸ１０１との間のデータの送受信を制御するインタフェースである。なお、第２ＬＡＮＩ／Ｆ２０４は、既存の全てのＩＦＡＸ１０１が備えるインタフェースと接続されるため、各機種の仕様等に限定されることなく既存のＩＦＡＸ１０１の全ての機種に接続することができる。これら２つのＬＡＮＩ／Ｆにより本ＡＤＰＴ１００は、ＩＦＡＸ１００とグループウェアネットワーク１０３との間で動作する。

【００４７】

バス２０５は、ＣＰＵ２００、ＲＯＭ２０１、ＲＡＭ２０２、第１ＬＡＮＩ／Ｆ２０３及び第２ＬＡＮＩ／Ｆ２０４間でデータが転送される経路である。

【００４８】

図４は、上記実施の形態に係るＡＤＰＴ１００の主要な機能を示すブロック図である。

【００４９】

信号種別判定部４００は、第２ＬＡＮＩ／Ｆ２０４を介してＩＦＡＸ１０１から出力されるコマンド信号の種別を判定する。そして、コマンド信号の種別に応じて、ＳＭＴＰ・ＰＯＰ３処理部４０１、ＨＴＴＰ処理部４０２及び電子メール通信部４０３にそのコマンド信号を受信した旨の通知をする。

【００５０】

ＳＭＴＰ・ＰＯＰ３処理部４０１は、信号種別判定部４００から通知を受けると、第２ＬＡＮＩ／Ｆ２０４を介してＩＦＡＸ１０１との間でＳＭＴＰプロトコル又はＰＯＰ３プロトコルに従って各種信号の通信を行う。

【００５１】

ＨＴＴＰ処理部４０２は、信号種別判定部４００から通知を受けると、第１ＬＡＮＩ／Ｆ２０３を介してグループウェアネットワーク１０３との間でＨＴＴＰプロトコルに従って、各種信号の通信を行う。

【００５２】

電子メール通信部４０３は、信号種別判定部４００から通知を受けると、第２ＬＡＮＩ／Ｆ２０４を介してＩＦＡＸ１０１との間で電子メールデータの通信を行う。ＩＦＡＸ１０１から電子メールを受信する場合、電子メール通信部４０３は、受信した電子メールデータをＲＡＭ２０２に格納する。一方、ＩＦＡＸ１０１に電子メールを送信する場合、電子メール通信部４０３は、ＲＡＭ２０２に格納された電子メールデータを取り出し、送信する。

【００５３】

ＨＴＭＬ通信部４０４は、第１ＬＡＮＩ／Ｆ２０３を介して、グループウェアネットワーク１０３との間でＨＴＭＬ文書データの通信を行う。

【００５４】

ＨＴＭＬ処理部４０５は、ＨＴＭＬ通信部４０４が受信したＨＴＭＬ文書データに所定のデータの書き込みを行う一方、ＲＡＭ２０２に格納された電子メール

データのＨＴＭＬ文書への変換処理を行う。

【００５５】

次に、上記構成を有するＡＤＰＴ１００が接続されたＩＦＡＸ１０１からグループウェアサーバ１０４に電子メールを送信する場合の処理について、図５に示すシーケンス図を参照しながら、図６に示すフロー図を用いて説明する。図５は、本実施の形態に係るＡＤＰＴ１００が接続されたＩＦＡＸ１０１からグループウェアサーバ１０４に電子メールを送信する場合のシーケンス図を示す。図６は、本実施の形態に係るＡＤＰＴ１００からグループウェアサーバ１０４に電子メールデータを送信する場合のフロー図を示す。

【００５６】

グループウェアサーバ１０４に電子メールを送信する場合、まず、ＩＦＡＸ１０１は、ＡＤＰＴ１００とのコネクション確立のための手順を実行する。すなわち、図５に示すように、ＩＦＡＸ１０１は、ＡＤＰＴ１００に対して、まず、同期を取るためのコマンド信号（ＳＹＮ）を送信する。そして、コマンド信号（ＳＹＮ）に応答してＡＤＰＴ１００から送信される、同期確認を示すコマンド信号（ＳＹＮ　ＡＣＫ）を受信し、ＩＦＡＸ１０１は、このコマンド信号（ＳＹＮ　ＡＣＫ）を受信したことを示すコマンド信号（ＡＣＫ）を送信する。この手順を実行することにより、ＩＦＡＸ１０１とＡＤＰＴ１００との間のコネクションが確立される。

【００５７】

ＩＦＡＸ１０１とＡＤＰＴ１００のコネクションが確立されると、ＡＤＰＴ１００は、グループウェアサーバ１０４とのコネクション確立のための手順を実行する。ＡＤＰＴ１００は、上述のＩＦＡＸ１０１が実行したのと同一の手順を実行する。この手順を実行することにより、ＡＤＰＴ１００とグループウェアサーバ１０４との間のコネクションが確立される。

【００５８】

ＡＤＰＴ１００とグループウェアサーバ１０４とのコネクションを確立する際に、最終確認となるコマンド信号（ＡＣＫ）をグループウェアサーバ１０４に送信すると、ＡＤＰＴ１００において、ＳＭＴＰ・ＰＯＰ３処理部４０１は、ＩＦ

ＡＸ１０１との間でＳＭＴＰプロトコルに従ってコマンド信号のやりとりを開始する。具体的には、まず、ＳＭＴＰ・ＰＯＰ３処理部４０１は、受信ＯＫを示す応答信号（２２０）をＩＦＡＸ１０１に対して出力する。

【００５９】

この”２２０”を受信すると、ＩＦＡＸ１０１は、通信路の使用開始宣言を示すコマンド信号（ＨＥＬＯ）をＡＤＰＴ１００に対して出力する。この”ＨＥＬＯ”を受信すると、ＡＤＰＴ１００において、信号種別判定部４００は、ＳＭＴＰ・ＰＯＰ３処理部４０１にその旨を通知する。この通知を受けると、ＳＭＴＰ・ＰＯＰ３処理部４０１は、受信ＯＫを示す応答信号（２５０）をＩＦＡＸ１０１に対して出力する。

【００６０】

そして、これ以降、ＩＦＡＸ１０１から出力されるメッセージの送信者名を示すコマンド信号（ＭＡＩＬ）、メッセージの宛先名を示すコマンド信号（ＲＣＰＴ）及びメッセージの送信開始を示すコマンド信号（ＤＡＴＡ）を受信して、ＳＭＴＰ・ＰＯＰ３処理部４０１は、各コマンド信号に対して、”２５０”、”２５０”及び”３５４”という応答信号をＩＦＡＸ１０１に出力する。なお、この”３５４”は、グループウェアサーバ１０４から後述する送信フォームを受け取ってからＩＦＡＸ１０１に出力される。

【００６１】

この”３５４”を受信した後、ＩＦＡＸ１０１から出力される電子メールデータ及び通信路の使用終了宣言を示すコマンド信号（ＱＵＩＴ）を受信する。そして、ＳＭＴＰ・ＰＯＰ３処理部４０１は、電子メールデータの受信完了時には”２５０”、”ＱＵＩＴ”に対しては”２２１”という応答信号をＩＦＡＸ１０１に出力する。これにより、ＩＦＡＸ１０１とＡＤＰＴ１００との間のコネクションが切断される。このように、ＩＦＡＸ１０１とＡＤＰＴ１００との間では、通常の電子メールデータのやりとりと同様に、ＳＭＴＰプロトコルに従って各種信号や電子メールデータのやりとりが行われる。

【００６２】

なお、電子メールデータの受信完了時に出力する”２５０”は、グループウェ

アサーバ１０４から後述する”ＰＯＳＴ”の応答信号を受信してからＩＦＡＸ１０１に出力される。

【００６３】

一方、ＩＦＡＸ１０１から”ＨＥＬＯ”を受信すると、ＡＤＰＴ１００において、信号種別判定部４００は、ＨＴＴＰ処理部４０２にその旨を通知する。この通知を受けると、ＨＴＴＰ処理部４０２は、グループウェアサーバ１０４との間でＨＴＴＰプロトコルに従ってコマンド信号のやりとりを開始する。具体的には、まず、ＨＴＴＰ処理部４０２は、接続を要求するコマンド信号（ＧＥＴ）をグループウェアサーバ１０４に対して出力する。これにより、ＨＴＴＰプロトコルに従ってグループウェアサーバ１０４と接続される（ＳＴ６０１）。

【００６４】

なお、ここでは、単にＨＴＴＰプロトコルに従って接続しているが、接続の際、ＳＳＬ（Secure Socket Layer）等の技術を用いてグループウェアサーバ１０４との間で交換されるデータのセキュリティを守るようにしても良い。

【００６５】

この”ＧＥＴ”を受信すると、グループウェアサーバ１０４は、応答信号として、認証要求を含むエラー信号をＡＤＰＴ１００に対して出力する。このエラー信号は、ヘッダとＨＴＭＬ文書データで構成され、そのＨＴＭＬ文書データに認証する方法が指定されている。これにより、グループウェアサーバ１０４から認証方法が指定される（ＳＴ６０２）。

【００６６】

このエラー信号を受信すると、ＨＴＴＰ処理部４０２は、送信フォームの要求を示すコマンド信号（ＧＥＴ）に予め設定されているユーザＩＤ（ＵＩＤ）及びパスワードを付与して送信する（ＳＴ６０３）。

【００６７】

この”ＧＥＴ”を受信すると、グループウェアサーバ１０４は、その”ＧＥＴ”に付与されたＵＩＤ及びパスワードが適正なものか判断し、適正である場合には送信フォームを含むデータ（以下、「送信フォームデータ」という）をＡＤＰＴ１００に対して出力する（ＳＴ６０４）。

【００６８】

図７は、グループウェアサーバ１０４から送信される送信フォームデータのソースデータを示している。図７に示すように、送信フォームデータは、ヘッダとＨＴＭＬ文書データで構成され、そのＨＴＭＬ文書データに送信フォームが含まれている。この送信フォームを受信することで、ＡＤＰＴ１００は、図８に示す送信フォームを認識することができる。なお、図８は、グループウェアサーバ１０４から送信される送信フォームの概念図である。

【００６９】

送信フォームデータを受信すると、ＡＤＰＴ１００において、ＨＴＭＬ通信部４０４は、この”ＤＡＴＡ”からＨＴＭＬ文書データで記述された送信フォームを抽出し、送信フォームを取得する（ＳＴ６０５）。このとき、ＨＴＴＰ処理部４０２は、この送信フォームデータを受信した旨を信号種別判定部４００に通知する。

【００７０】

送信フォームデータを受信した旨の通知を受けると、信号種別判定部４００は、ＳＭＴＰ・ＰＯＰ３処理部４０１にその旨を通知する。この通知を受けると、上述のように、ＡＤＰＴ１００において、ＳＭＴＰ・ＰＯＰ３処理部４０１は、”３５４”という応答信号をＩＦＡＸ１０１に送信し、ＩＦＡＸ１０１からの電子メールデータの送信を促す。そして、ＩＦＡＸ１０１から送信された電子メールデータを電子メール通信部４０３が受信し、ＲＡＭ２０２に格納する（ＳＴ６０６）。

【００７１】

ＨＴＭＬ処理部４０５は、ＲＡＭ２０２に格納された電子メールデータから送信先（図８に示す「To」）、件名（図８に示す「Subject」）、ファイル名（図８に示す「File Name」）を抽出し、受信した送信フォームの所定位置に書き込む。そして、この送信フォームをＨＴＭＬ通信部４０４に渡す。ＨＴＭＬ通信部４０４は、この送信フォームを含むコマンド信号（ＰＯＳＴ）をグループウェアサーバ１０４に送信すると共に電子メールデータをグループウェアサーバ１０４に送信する（ＳＴ６０７）。

【００７２】

図９は、ＡＤＰＴ１００が送信する”ＰＯＳＴ”のソースデータを示している。図９に示すように、”ＰＯＳＴ”は、ヘッダと送信データで構成され、その送信データに上述の送信フォームに書き込まれる所定情報が含まれている。具体的には、図９に示すように、送信先（ａｂｃ＠ｄｅｆ．ｃｏｍ）、件名（ｔｅｓｔ）及びファイル名（￥￥ｉｍａｇｅ．ｔｉｆ）が記述されている。この”ＰＯＳＴ”を受信することで、グループウェアサーバ１０４は、図１０に示す所定情報が書き込まれた送信フォームを認識することができる。なお、図１０は、ＡＤＰＴ１００から送信される送信データが記述された送信フォームの概念図である。

【００７３】

このような”ＰＯＳＴ”及び電子メールデータを受信すると（ＳＴ６０８）、送信フォームに記述された情報に従って、グループウェアサーバ１０４は、ＣＧＩ処理を起動し（ＳＴ６０９）、送信フォームに記述された送信先の電子メールアドレスの検証を行う（ＳＴ６１０）。具体的には、その送信先の電子メールアドレスがグループウェアネットワーク１０３上のクライアント端末かどうかを判定する。ここで、グループウェアネットワーク１０３上のクライアント端末である場合には、電子メールデータは、該当するメールボックスに格納される（ＳＴ６１１）。一方、グループウェアネットワーク１０３上のクライアント端末でない場合には、電子メールデータは、インターネット１０８を介して他のメールサーバに転送される（ＳＴ６１２）。

【００７４】

その後、グループウェアサーバ１０４は、電子メールデータの受信処理の終了を示すため、”ＰＯＳＴ”の応答信号をＡＤＰＴ１００に出力する。これにより、グループウェアサーバ１０４とＡＤＰＴ１００との間のコネクションが切断される。このように、グループウェアサーバ１０４とＡＤＰＴ１００との間では、ＩＦＡＸ１０１からの”ＨＥＬＯ”の受信をきっかけにして、ＨＴＴＰプロトコルに従って各種信号や電子メールデータのやりとりが行われる。

【００７５】

このように本実施の形態のＡＤＰＴ１００によれば、ＩＦＡＸ１０１からグル

ープウェアサーバ１０４に電子メールを送信する際、ＩＦＡＸ１０１との間でＳＭＴＰプロトコルに従って各種信号や電子メールデータの通信を行う一方、グループウェアサーバ１０４との間でＨＴＴＰプロトコルに従って各種信号や電子メールデータの通信を行う。このため、ＨＴＴＰプロトコルに従って通信が行われるグループウェアネットワーク１０３においても、ＩＦＡＸ１０１は、正常に電子メールの送信動作を行うことができる。

【００７６】

また、本実施のＡＤＰＴ１００によれば、グループウェアサーバ１０４から送信フォームデータを受信した後、ＩＦＡＸ１０１に対して”３５４”を送信する。そして、ＩＦＡＸ１０１から電子メールデータを受信した後、送信先等の情報を記述して送信フォームをグループウェアサーバ１０４に送信する。このため、送信フォームを認識する前に電子メールデータがＩＦＡＸ１０１から送信され、電子メールデータの受信から長時間が経過することによるＡＤＰＴ１００での誤動作を防止することができる。これにより、確実に電子メールの送信動作を行うことができる。

【００７７】

次に、ＡＤＰＴ１００が接続されたＩＦＡＸ１０１がグループウェアサーバ１０４から電子メールを受信する場合の処理について、図１１に示すシーケンス図を参照しながら、図１２に示すフロー図を用いて説明する。図１１は、本実施の形態に係るＡＤＰＴ１００が接続されたＩＦＡＸ１０１がグループウェアサーバ１０４から電子メールを受信する場合のシーケンス図を示す。図１２は、本実施の形態に係るＡＤＰＴ１００がグループウェアサーバ１０４から電子メールデータを受信する場合のフロー図を示す。

【００７８】

グループウェアサーバ１０４から電子メールを受信する場合においても、グループウェアサーバ１０４に電子メールを送信する場合と同様に、ＩＦＡＸ１０１は、まず、ＡＤＰＴ１００とのコネクション確立のための手順を実行する。また、ＩＦＡＸ１０１とＡＤＰＴ１００のコネクションが確立されると、ＡＤＰＴ１００も、グループウェアサーバ１０４に電子メールを送信する場合と同様に、グ

ループウェアサーバ１０４とのコネクション確立のための手順を実行する。

【００７９】

ＡＤＰＴ１００とグループウェアサーバ１０４とのコネクションを確立する際に、最終確認となるコマンド信号（ＡＣＫ）をグループウェアサーバ１０４に送信すると、ＡＤＰＴ１００において、ＳＭＴＰ・ＰＯＰ３処理部４０１は、ＩＦＡＸ１０１との間でＰＯＰ３プロトコルに従ってコマンド信号のやりとりを開始する。具体的には、まず、ＳＭＴＰ・ＰＯＰ３処理部４０１は、肯定応答を示すＯＫレスポンスをＩＦＡＸ１０１に対して出力する。

【００８０】

このＯＫレスポンスを受信すると、ＩＦＡＸ１０１は、メールボックス名の送信を示すコマンド信号（ＵＳＥＲ）をＡＤＰＴ１００に対して出力する。この”ＵＳＥＲ”を受信すると、ＡＤＰＴ１００において、信号種別判定部４００は、ＳＭＴＰ・ＰＯＰ３処理部４０１にその旨を通知する。この通知を受けると、ＳＭＴＰ・ＰＯＰ３処理部４０１は、肯定応答を示すＯＫレスポンスをＩＦＡＸ１０１に対して出力する。

【００８１】

そして、これ以降、ＳＭＴＰ・ＰＯＰ３処理部４０１は、ＩＦＡＸ１０１から出力されるメールボックス・パスワードの送信を示すコマンド信号（ＰＡＳＳ）、受信状態の問い合わせを示すコマンド信号（ＳＴＡＴ）、メールのダウンロード要求を示すコマンド信号（ＲＥＴＲ）を受信して、各コマンド信号に対して、肯定応答として、ＯＫレスポンスをＩＦＡＸ１０１に出力する。

【００８２】

なお、”ＳＴＡＴ”を受信した後、ＩＦＡＸ１０１に出力するＯＫレスポンスには、受信する電子メールデータの数及び各電子メールデータの容量が含まれる。また、ＩＦＡＸ１０１から受信した”ＲＥＴＲ”とこれに対する肯定応答としてＩＦＡＸ１０１に出力するＯＫレスポンスの間に、ＡＤＰＴ１００は、リンク先情報を含むコマンド信号（ＧＥＴ）をグループウェアサーバ１０４に送信すると共に、グループウェアサーバ１０４から送信される電子メールデータを受信する。

【００８３】

そして、”ＲＥＴＲ”に対する肯定応答として、ＯＫレスポンスをＩＦＡＸ１０１に出力した後、ＡＤＰＴ１００は、電子メールデータをＩＦＡＸ１０１に出力する。

【００８４】

一方、ＩＦＡＸ１０１から”ＵＳＥＲ”を受信すると、ＡＤＰＴ１００において、信号種別判定部４００は、ＨＴＴＰ処理部４０２にその旨を通知する。この通知を受けると、ＨＴＴＰ処理部４０２は、グループウェアサーバ１０４との間でＨＴＴＰプロトコルに従ってコマンド信号のやりとりを開始する。具体的には、まず、ＨＴＴＰ処理部４０２は、接続を要求するコマンド信号（ＧＥＴ）をグループウェアサーバ１０４に対して出力する。これにより、ＨＴＴＰプロトコルに従ってグループウェアサーバ１０４と接続される（ＳＴ１２０１）。

【００８５】

この”ＧＥＴ”を受信すると、グループウェアサーバ１０４は、応答信号として、認証要求を含むエラー信号をＡＤＰＴ１００に対して出力する。このエラー信号は、ヘッダとＨＴＭＬ文書データで構成され、そのＨＴＭＬ文書データに認証する方法が指定されている。これにより、グループウェアサーバ１０４から認証方法が指定される（ＳＴ１２０２）。

【００８６】

このエラー信号を受信すると、ＨＴＴＰ処理部４０２は、受信フォームの要求を示すコマンド信号（ＧＥＴ）に予め設定されているユーザＩＤ（ＵＩＤ）及びパスワードを付与して送信する（ＳＴ１２０３）。

【００８７】

この”ＧＥＴ”を受信すると、グループウェアサーバ１０４は、その”ＧＥＴ”に付与されたＵＩＤ及びパスワードが適正なものか判断し、適正である場合に応答信号として、受信フォームを含むデータ（以下、「受信フォームデータ」という）をＡＤＰＴ１００に対して出力する（ＳＴ１２０４）。

【００８８】

図１３は、グループウェアサーバ１０４から送信される受信フォームデータの

ソースデータを示している。図１３に示すように、受信フォームデータは、ヘッダとＨＴＭＬ文書データで構成され、そのＨＴＭＬ文書データに受信フォームが含まれている。この受信フォームを受信することで、ＡＤＰＴ１００は、例えば、図１４に示す受信フォームを認識することができる。なお、図１４は、グループウェアサーバ１０４から送信される受信フォームの概念図である。

【００８９】

受信フォームデータを受信すると、ＡＤＰＴ１００において、ＨＴＭＬ通信部４０４は、この受信フォームデータからＨＴＭＬ文書データで記述された受信フォームを抽出し、受信フォームを取得する（ＳＴ１２０５）。このとき、ＨＴＴＰ処理部４０２は、この受信フォームデータを受信した旨を信号種別判定部４００に通知する。

【００９０】

受信フォームデータを受信した旨の通知を受けると、信号種別判定部４００は、ＳＭＴＰ・ＰＯＰ３処理部４０１にその旨を通知する。この通知を受けると、ＳＭＴＰ・ＰＯＰ３処理部４０１は、ＨＴＭＬ文書データで記述された受信フォームの中からＨＴＭＬ処理部４０５が抽出した電子メールデータの数及び各電子メールデータの容量を”ＳＴＡＴ”に対するＯＫレスポンスに付与して、ＩＦＡＸ１０１に送信する。

【００９１】

受信フォームを取得すると、ＡＤＰＴ１００において、その受信フォームから新規の電子メールデータの有無が判断される（ＳＴ１２０６）。ここで、新規の電子メールデータがない場合には、ＩＦＡＸ１０１における電子メールの受信処理が終了する（ＳＴ１２０７）。

【００９２】

一方、新規の電子メールデータがある場合には、その受信データを指定した受信フォーム、言い換えると、リンク先が指定された受信フォームを含むコマンド信号（ＧＥＴ）をグループウェアサーバ１０４に送信する（ＳＴ１２０８）。ここでは新規の電子メールデータがあるものとする。

【００９３】

図１５は、ＡＤＰＴ１００が送信する受信フォームを含む”ＧＥＴ”のソースデータを示している。図１５に示す受信フォームを含む”ＧＥＴ”を受信することで、グループウェアサーバ１０４は、図１４に示す上側の電子メールデータの受信要求を認識することができる。

【００９４】

このような”ＧＥＴ”を受信すると（ＳＴ１２０９）、グループウェアサーバ１０４は、その”ＧＥＴ”に対応する電子メールデータをＡＤＰＴ１００に対して送信する（ＳＴ１２１０）。

【００９５】

このとき、グループウェアサーバ１０４から送信される電子メールデータは、ＨＴＭＬ文書データで記述されている。ＨＴＭＬ通信部４０４は、この電子メールデータを受信する（ＳＴ１２１１）。そして、ＨＴＭＬ処理部４０５は、このＨＴＭＬ文書で記述された電子メールデータからＴＩＦＦファイルを抽出し（ＳＴ１２１２）、ＲＡＭ２０２にそのＴＩＦＦファイルを格納する。

【００９６】

ＲＡＭ２０２にＴＩＦＦファイルが格納されると、電子メール通信部４０３は、そのＴＩＦＦファイルを取り出して、ＩＦＡＸ１０１に転送する（ＳＴ１２１３）。

【００９７】

そして、電子メールデータを転送した後、図１１に示すように、ＩＦＡＸ１０１から出力される電子メールの削除要求を示すコマンド信号（ＤＥＬＥ）を受信する。この”ＤＥＬＥ”を受信すると、受信フォームに記述された電子メールのうち、既にダウンロードした電子メールデータの削除を要求する受信フォームを含むコマンド信号（ＰＯＳＴ）をグループウェアサーバ１０４に出力する。ここでは、図１４に示す上側の電子メールデータのダウンロードを終了しているため、この電子メールデータの削除を要求する。

【００９８】

図１６は、ＡＤＰＴ１００が出力する受信フォームを含む”ＰＯＳＴ”のソースデータを示している。図１６に示すように、この”ＰＯＳＴ”は、ヘッダと送

信データとで構成される。ヘッダには、削除を要求する電子メールデータを識別するための情報が含まれており、送信データには、図１４の概念図で示した削除チェックボックスにチェックを入れるためのデータが含まれている。

【００９９】

このような”ＰＯＳＴ”を受信すると、グループウェアサーバ１０４は、指定された電子メールデータを削除するためのＣＧＩ処理を起動し、その電子メールデータの削除処理を行う。そして、指定された電子メールデータの削除処理を行った後、グループウェアサーバ１０４は、削除処理を行った後に残った電子メールデータを含む受信フォームを再度、ＡＤＰＴ１００に送信する。ここでは、図１４に示す下側の電子メール情報だけが含まれる受信フォームがＡＤＰＴ１００に送信される。

【０１００】

この受信フォームを受信した後、ＡＤＰＴ１００は、上述の”ＤＥＬＥ”に対する肯定応答として、ＯＫレスポンスを出力する。そして、このＯＫレスポンスを受信したＩＦＡＸ１０１は、上述した要領で、”ＲＥＴＲ”をＡＤＰＴ１００に出力することで、次の電子メールデータのダウンロード要求をする。ここでは、図１４に示す下側の電子メールデータのダウンロードが要求されることとなるが、上述の説明と同様の処理であるため、説明を省略する。

【０１０１】

そして、受信フォームに含まれる全ての電子メールデータのダウンロードを終了後、”ＤＥＬＥ”をＡＤＰＴ１００に出力し、ＡＤＰＴ１００からこの肯定応答としてＯＫレスポンスを受信すると、ＩＦＡＸ１０１は、完了通知を示すコマンド信号（ＱＵＩＴ）を送信する。

【０１０２】

ＡＤＰＴ１００は、この”ＱＵＩＴ”を受信し、これに対する肯定応答としてＯＫレスポンスを出力する。これにより、ＩＦＡＸ１０１とＡＤＰＴ１００との間のコネクションが切断される。

【０１０３】

このように、ＩＦＡＸ１０１とＡＤＰＴ１００との間では、通常の電子メール

データのやりとりと同様に、ＰＯＰ３プロトコルに従って各種信号や電子メールデータのやりとりが行われる。一方、ＡＤＰＴ１００とグループウェアサーバ１０４との間では、ＩＦＡＸ１０１からの”ＵＳＥＲ”の受信をきっかけとしてＨＴＴＰプロトコルに従って各種信号や電子メールデータのやりとりが行われる。

【０１０４】

このように本実施の形態のＡＤＰＴ１００によれば、ＩＦＡＸ１０１がグループウェアサーバ１０４から電子メールを受信する際、ＩＦＡＸ１０１との間でＰＯＰ３プロトコルに従って各種信号や電子メールデータの通信を行う一方、グループウェアサーバ１０４との間でＨＴＴＰプロトコルに従って各種信号や電子メールデータの通信を行う。このため、ＨＴＴＰプロトコルに従って通信が行われるグループウェアネットワーク１０３においても、ＩＦＡＸ１０１は、正常に電子メールの受信動作を行うことができる。

【０１０５】

（実施の形態２）

図１７は、本発明の実施の形態２に係るＡＤＰＴ１００のハードウエア構成を示すブロック図である。図１７において、図３と同一の符号が付されている構成については、同一の機能を有するものとし説明を省略する。

【０１０６】

図１７に示すように、実施の形態２に係るＡＤＰＴ１００は、実施の形態１に係るＡＤＰＴ１００の構成に加え、所定のＩＣカード１７０１に所定データの書込み、あるいは、ＩＣカード１７０１に書き込まれたデータの読取りを行うＩＣカードＲＥＡＤ／ＷＲＩＴＥ部（以下、「ＩＣカードＲ／Ｗ部」という）１７０２を具備する。

【０１０７】

ＩＣカード１７０１は、本ＡＤＰＴ１００が接続されたＩＦＡＸ１０１から電子メールの送受信を行うユーザに予め配布されているものである。なお、ＩＣカード１７０１に書き込まれたデータの詳細については後述する。

【０１０８】

図１８は、実施の形態２に係るＡＤＰＴ１００の主要な機能を示すブロック図

である。なお、図１８において、図４と同一の符号が付されている構成要素については、同一の機能を有するものとし説明を省略する。

【０１０９】

カード情報判定部１８０１は、ＩＣカードスロット１７０２Ａに装着されたＩＣカード１７０１からＩＣカードＲ／Ｗ部１７０２が読み取った情報の内容を判定する。そして、ＩＣカード１７０１に署名処理又は署名暗号化処理に必要な情報が格納されている場合に署名暗号化処理部１８０２にその情報を与える。

【０１１０】

また、カード情報判定部１８０１は、ＩＣカードＲ／Ｗ部１７０２が読み取った情報に基いてＩＣカード１７０１の装着の有無についても判定する。さらに、カード情報判定部１８０１は、ＩＣカード１７０１に格納された電子メールアドレス情報を判定し、その電子メールアドレス情報を電子メール通信部４０３に通知する。

【０１１１】

署名暗号化処理部１８０２は、カード情報判定部１８０１から受け取った署名暗号化処理等に必要な情報に基いて、電子メール通信部４０３がＩＦＡＸ１０１から受信した電子メールデータに対して署名暗号化処理等の処理を行う。また、署名暗号化処理部１８０２は、カード情報判定部１８０１から受け取った署名暗号化処理等に必要な情報に基いて、電子メール通信部４０３がグループウェアネットワーク１０３から受信した電子メールデータに施された署名暗号化処理等の解読処理を行う。

【０１１２】

ここで、ＩＣカード１７０１に格納された情報について説明する。

【０１１３】

ＩＣカード１７０１は、上述のように、ＩＦＡＸ１０１を用いて電子メール通信を行う各ユーザに配布されるものであり、各ユーザに付与された電子メールアドレス情報が格納されている。すなわち、ＡＤＰＴ１００にＩＣカード１７０１が装着されているときのみ、各ユーザは、自分の電子メールアドレスから電子メールを送信することができ、自分の電子メールアドレスに対する電子メールを受

信することができる。

【０１１４】

また、ＩＣカード１７０１は、署名処理又は署名暗号化処理に必要となる情報を格納する。すなわち、ＩＣカード１７０１は、自分の秘密鍵情報及び公開鍵情報を格納する。なお、送信先の公開鍵情報は、ＡＤＰＴ１００のＲＡＭ２０２内に蓄積されている。

【０１１５】

次に、以上のような構成を有するＡＤＰ１００が接続されたＩＦＡＸ１０１からグループウェアサーバ１０４に電子メールを送信する場合の処理について、図５に示すシーケンス図を参照しながら、図１９に示すフロー図を用いて説明する。図１９は、実施の形態２に係るＡＤＰＴ１００がＩＦＡＸ１０１から受信した電子メールデータに対する署名暗号化処理等の処理を示すフロー図である。なお、ＩＦＡＸ１０１から送信する電子メールデータには全て暗号化処理が施されるものとする。

【０１１６】

実施の形態２においても、ＩＦＡＸ１０１からグループウェアサーバ１０４に電子メールを送信する場合、実施の形態１で図５を用いて説明した場合と同様に、ＩＦＡＸ１０１とＡＤＰＴ１００の間においてＳＭＴＰプロトコルに従って各種信号のやりとりが行われ、その後に電子メールデータを受信する。受信した電子メールデータは、以下に説明するように暗号化処理が施される一方、後述する送信フォームへの所定データの書込み処理が終了するまでオリジナルの電子メールデータがＲＡＭ２０２に保持される。

【０１１７】

ＩＦＡＸ１０１から電子メールデータを受信すると（ＳＴ１９０１）、カード情報判定部１８０１は、ＩＣカードＲ／Ｗ部１７０２が読み取った情報に基づいて、ＩＣカード１７０１がＡＤＰＴ１００のスロット１７０２Ａに挿入されているか判定する（ＳＴ１９０２）。

【０１１８】

ここで、ＩＣカード１７０１がＡＤＰＴ１００のスロット１７０２Ａに挿入さ

れていない場合には、ＡＤＰＴ１００では、通常の電子メールの送信処理が行われる（ＳＴ１９０３）。すなわち、ＩＦＡＸ１０１に付与された電子メールアドレスから電子メールの送信処理が行われる。

【０１１９】

一方、ＩＣカード１７０１が本ＡＤＰＴ１００のスロット１７０２Ａに挿入されている場合には、ＩＣカードＲ／Ｗ部１７０２は、ＩＣカード１７０１からこのユーザに関する情報（以下、「ユーザ情報」という）を抽出する。このとき、このユーザの電子メールアドレス情報が抽出される（ＳＴ１９０４）。

【０１２０】

そして、カード情報判定部１８０１は、ＩＣカードＲ／Ｗ部１７０２が抽出したユーザ情報から電子メールアドレス情報を判定し、電子メール通信部４０３に通知する。電子メール通信部４０３は、その電子メールアドレス情報を電子メールの送信元情報に設定する（ＳＴ１９０５）。具体的にいうと、抽出された電子メールアドレス情報が電子メールのヘッダ情報の［Ｆｒｏｍ：］に設定される。

【０１２１】

電子メールの送信元情報が設定されると、本ＡＤＰＴ１００において、Ｓ／ＭＩＭＥ処理が施される。まず、本ＡＤＰＴ１００において、送信先情報があるか判定される（ＳＴ１９０６）。具体的には、本ＡＤＰＴ１００のＲＡＭ２０２に送信先の公開鍵情報が格納されているかが判定される。

【０１２２】

ここで、送信先情報がない場合には、カード情報判定部１８０１は、ＩＣカードＲ／Ｗ部１７０２が抽出したユーザ情報から自己の秘密鍵情報を判定し、署名暗号化処理部１８０２に渡す。署名暗号化処理部１８０２は、この自己の秘密鍵情報を用いて署名処理を行う（ＳＴ１９０７）。

【０１２３】

具体的には、電子メールデータのメッセージデータからハッシュ関数等の不可逆性の関数で演算処理を行い、メッセージダイジェストを取り出し、そのメッセージダイジェストに自己の秘密鍵情報を用いて暗号化処理を施す。

【０１２４】

一方、送信先情報がある場合には、署名暗号化処理部１８０２は、この送信先の公開鍵情報を入手する。一方、カード情報判定部１８０１は、ＩＣカードＲ／Ｗ部１７０２が抽出したユーザ情報から自己の秘密鍵情報を署名暗号化処理部１８０２に渡す。署名暗号化処理部１８０２は、この自己の秘密鍵情報及び送信先の公開鍵情報を用いて署名暗号化処理を行う（ＳＴ１９０８）。

【０１２５】

具体的には、まず、上述のように電子メールのメッセージからハッシュ関数等の不可逆性の関数で演算処理を行い、メッセージダイジェストを取り出し、そのメッセージダイジェストに自己の秘密鍵情報を用いて暗号化処理を施す。さらに、ＤＥＫ（Data Encryption Key）と呼ばれる擬似乱数を用いた暗号鍵を生成する。そして、そのＤＥＫに対して送信先の公開鍵情報を用いて暗号化処理を施す。一方、先に暗号化処理を施したメッセージダイジェスト（署名結果）及び電子メールのメッセージデータに対して、そのＤＥＫで所定の暗号化方式（例えば、ＤＥＳ：Data Encryption Standard等）にしたがって暗号化処理を施す。

【０１２６】

そして、ＳＴ１９０７又はＳＴ１９０８で署名暗号化処理等を施した後、署名暗号化処理部１８０２は、その電子メールデータをＲＡＭ２０２に格納する（ＳＴ１９０９）。

【０１２７】

署名暗号化処理後の電子メールデータがＲＡＭ２０２に格納されると、図５で説明した場合と同様に、ＨＴＭＬ処理部４０５は、ＲＡＭ２０２に格納されたオリジナルの電子メールデータから送信先（図８に示す「To」）、件名（図８に示す「Subject」）、ファイル名（図８に示す「File Name」）を抽出し、受信した送信フォームの所定位置に書き込む。そして、この送信フォームをＨＴＭＬ通信部４０４に渡す。ＨＴＭＬ通信部４０４は、この送信フォームを含むコマンド信号（ＰＯＳＴ）をグループウェアサーバ１０４に送信すると共に署名暗号化処理が施された電子メールデータをＲＡＭ２０２から取り出し、グループウェアサーバ１０４に送信する。このようにしてＡＤＰＴ１００がＩＦＡＸ１０１から受信した電子メールデータに対する署名暗号化等の処理を終了する。

【０１２８】

このように本実施の形態のＡＤＰＴ１００によれば、ＩＦＡＸ１０１から電子メールデータを送信する際、ＨＴＴＰプロトコルに従って通信が行われるグループウェアネットワーク１０３においても、ＩＦＡＸ１０１に正常に電子メールの送信動作を行わせることができるだけでなく、必要に応じてその電子メールデータに暗号化処理を施すことができるので、既存のＩＦＡＸに特別な構成を附加することなく、電子メールの秘匿性を確保することができる。

【０１２９】

また、電子メールに暗号化処理を施す際、本ＡＤＰＴ１００は、各ユーザに配布されたＩＣカード１７０１の有無を判定し、暗号化処理の要否を判断する。これにより、暗号化処理を行う必要がない電子メールデータは、暗号化処理を施すことなく送信できる一方、暗号化処理を行う必要がある電子メールデータは、暗号化処理を施して送信することできるので、簡単に暗号化処理の要否を判断することができる。

【０１３０】

さらに、電子メールに暗号化処理を施す際、本ＡＤＰＴ１００は、挿入されたＩＣカード１７０１内に格納された暗号化処理に必要な情報を用いて暗号化処理を施す。各ユーザが管理するＩＣカード１７０１に格納された情報を用いて暗号化処理が行なわれるため、その情報の書き換え等を防止することができる。

【０１３１】

次に、本ＡＤＰＴ１００が接続されたＩＦＡＸ１０１がグループウェアサーバ１０４から電子メールを受信する場合の処理について、図１１に示すシーケンス図を参照しながら、図２０に示すフロー図を用いて説明する。図２０は、ＡＤＰＴ１００がグループウェアサーバ１０４から電子メールデータを受信し、その電子メールデータに施された署名暗号化処理等の解読を行うの処理を示すフロー図である。なお、図２０において、図１２と同一の符号については、同一の処理を行うものとする。また、グループウェアサーバ１０４から受信する電子メールは、全て暗号化処理が施されているものとする。

【０１３２】

実施の形態２においても、グループウェアサーバ１０４から電子メールデータを受信する場合、実施の形態１で図１１を用いて説明した場合と同様に、ＩＦＡＸ１０１がまず、ＡＤＰＴ１００とのコネクション確立のための手順を実行する。このとき、ＡＤＰＴ１００は、このコネクション確立のために最初に送信される”ＳＹＮ”を電子メールの受信指示として捉える。これにより、ＡＤＰＴ１００において、この受信指示があるかが判定される（ＳＴ２００１）。

【０１３３】

電子メールの受信指示があると判定されると、カード情報判定部１８０１は、ＩＣカードＲ／Ｗ部１７０２が読み取った情報に基づいてＩＣカード１７０１がＡＤＰＴ１００のスロット１７０２Ａに挿入されているか判定する（ＳＴ２００２）。

【０１３４】

ここで、ＩＣカード１７０１がＡＤＰＴ１００のスロット１７０２Ａに挿入されていない場合には、ＡＤＰＴ１００では、ＩＦＡＸ１０１から指示したユーザの電子メールアドレス情報を確認することができないため、電子メールの受信処理は行われない（ＳＴ２００３）。

【０１３５】

一方、ＩＣカード１７０１がＡＤＰＴ１００のスロット１７０２Ａに挿入されている場合には、図１１で説明したように、所定のコマンド信号及び応答信号が交換され、ＩＦＡＸ１０１とＡＤＰＴ１００との間、ＡＤＰＴ１００とグループウェアサーバ１０４との間のコネクションが確立される。そして、双方のコネクションが確立された後、図１１で説明したのと同様の要領でＡＤＰＴ１００は、ＨＴＴＰプロトコルに従ってグループウェアサーバ１０４と接続する（ＳＴ１２０１）。

【０１３６】

ＨＴＴＰプロトコルに従ってＡＤＰＴ１００と接続後、グループウェアサーバ１０４から認証要求を含むエラー信号を受信すると、ＡＤＰＴ１００において、ＨＴＴＰ処理部４０２は、予め設定されたＵＩＤ及びパスワード受信フォームの要求を示すコマンド信号（ＧＥＴ）に付与して送信する（ＳＴ１２０３）。

【０１３７】

この”ＧＥＴ”を受信すると、ＳＴ１２０４において、所定の場合にグループウェアサーバ１０４から応答信号として出力される、受信フォームデータを受信する。そして、ＡＤＰＴ１００において、ＨＴＭＬ通信部４０４は、この受信フォームデータからＨＴＭＬ文書データで記述された受信フォームを抽出し、受信フォームを取得する（ＳＴ１２０５）。

【０１３８】

受信フォームを取得すると、ＡＤＰＴ１００において、その受信フォームから新規の電子メールデータの有無が判断され（ＳＴ１２０６）、新規の電子メールデータがある場合、リンク先が指定された受信フォームを含むコマンド信号（ＧＥＴ）をグループウェアサーバ１０４に送信する（ＳＴ１２０８）。

【０１３９】

この”ＧＥＴ”を受信すると（ＳＴ１２０９）、ＳＴ１２１０においてグループウェアサーバ１０４から出力される、その”ＧＥＴ”に対応する、ＨＴＭＬ文書データで記述された電子メールデータをＨＴＭＬ通信部４０４が受信する（ＳＴ１２１１）。そして、ＨＴＭＬ処理部４０５は、このＨＴＭＬ文書で記述された電子メールデータからＴＩＦＦファイルを抽出し（ＳＴ１２１２）、ＲＡＭ２０２にそのＴＩＦＦファイルを格納する。なお、このとき、ＴＩＦＦファイルには暗号化処理が施されている。

【０１４０】

ＲＡＭ２０２にＴＩＦＦファイルが格納されると、ＡＤＰＴ１００において、送信者情報があるかが判定される（ＳＴ２００４）。具体的には、ＡＤＰＴ１００に送信者の公開鍵情報が格納されているかが判定される。なお、この公開鍵情報は、電子メールのメッセージダイジェストの暗号化を解読する際に用いられるものである。

【０１４１】

送信者の公開鍵情報がない場合には、その電子メールに付与された送信者の公開鍵情報をＡＤＰＴ１００のＲＡＭ２０２に格納する（ＳＴ２００５）。そして、署名暗号化処理部１８０２は、その電子メールデータが暗号化されているか判

定する（ＳＴ２００６）。一方、送信者の公開鍵情報がある場合には、さらにその公開鍵情報を格納することなく、直接、その電子メールデータが暗号化されているか判定する（ＳＴ２００６）。

【０１４２】

ここでは、電子メールデータが暗号化されているため、ＲＡＭ２０２からそのＴＩＦＦファイルを取り出し、署名暗号化処理部１８０２は、そのＴＩＦＦファイルの復号化処理を行う（ＳＴ２００７）。

【０１４３】

具体的には、暗号化されているＤＥＫを自分の秘密鍵情報で復号化し、復号化したＤＥＫで暗号化されたデータを復号化する。そして、復号化したデータから、電子メールデータをメッセージダイジェストとメッセージデータに分離する。その際、メッセージダイジェストを送信者の公開鍵情報で復号化し、その結果を保持しておく。一方、分離したメッセージデータから、上述したようなハッシュ関数を用いてメッセージダイジェストを抽出する。そして、そこで得たメッセージダイジェストと先ほど保持したメッセージダイジェストとを比較する。これにより、電子メールのメッセージデータが改ざんされていないか、また、正当な送信者から送信されたかを確認することができる。

【０１４４】

なお、メッセージデータが暗号化されていないような場合には、署名暗号化処理部１８０２は、そのメッセージダイジェストのみ復号化し、正当な送信者から送信されたかだけを確認する。

【０１４５】

そして、署名暗号化処理部１８０２は、このように復号化したＴＩＦＦファイルをＲＡＭ２０２に格納する（ＳＴ２００８）。復号化処理後のＴＩＦＦファイルがＲＡＭ２０２に格納されると、図１１で説明したのと同様に、電子メール通信部４０３は、そのＴＩＦＦファイルを取り出して、ＩＦＡＸ１０１に転送する（ＳＴ１２１３）。このようにしてＡＤＰＴ１００がグループウェアサーバ１０４から受信した電子メールデータを復号化する処理が終了する。

【０１４６】

このように本実施の形態のＡＤＰＴ１００によれば、グループウェアサーバ１０４から電子メールを受信する際、ＨＴＴＰプロトコルに従って通信が行われるグループウェアネットワーク１０３においても、ＩＦＡＸ１０１に正常に電子メールの受信動作を行わせることができるだけでなく、その電子メールに暗号化処理が施されているか判断し、施されている場合にはその暗号化処理された電子メールデータを復号化し、ＩＦＡＸ１０１に転送する。このため、既存のＩＦＡＸに特別な構成を附加することなく、電子メールの秘匿性を確保して電子メールを受信することができる。

【０１４７】

また、電子メールの受信処理を行う際、ＡＤＰＴ１００は、各ユーザに配布されたＩＣカード１７０１の装着の有無を判定し、そのＩＣカード１７０１がない場合には、電子メールの受信処理を行わない。このため、電子メールの受信の際に受信者の認証を行うことができる。したがって、単一のＩＦＡＸ１０１を用いた場合でも、他の人に自分宛ての電子メールデータを見られるという事態を防止することができる。

【０１４８】

なお、本実施の形態では、ＡＤＰＴ１００の挿入されるＩＣカード１７０１は、署名暗号化に必要な情報等を格納するメモリカードのような構成を有している。しかし、ＩＣカード１７０１の構成としては、これに限定されず、例えば、ＩＣカード１７０１に署名暗号化処理のプログラム等を内蔵し、署名暗号化処理の一部又は全部をＩＣカード１７０１内で行うようにしても良い。この場合には、例えば、本ＡＤＰＴ１００から処理すべき、暗号化されたメッセージダイジェスト（ハッシュ値）又は暗号化されたＤＥＫを受け取って所定の暗号化処理又は復号化処理の一部をＩＣカード１７０１内で行うことができる。所定のデータを受け取って暗号化処理等の処理が行われるため、暗号化処理等の処理に必要な情報を単に格納する場合と比べて、暗号化処理等に必要な情報が他人により読み取られるのをより確実に防止することができる。

【０１４９】

また、本実施の形態では、ＩＣカード１７０１に暗号化処理等に必要な情報を

格納し、その暗号化処理等の処理を行う暗号化処理装置１００について説明している。しかし、これに限定されず、暗号化処理等に必要な情報は、暗号化処理装置１００のメモリ等に格納しておいてももちろん良い。このように変更した場合にも、本実施の形態と同様の効果を得ることができる。

【０１５０】

【発明の効果】

以上説明したように本発明によれば、ＩＦＡＸとグループウェアサーバとの間で電子メール通信を行う際、ＩＦＡＸとの間でＳＭＴＰプロトコル又はＰＯＰ３プロトコルに従って各種信号や電子メールデータの通信を行う一方、グループウェアサーバとの間でＨＴＴＰプロトコルに従って各種信号や電子メールデータの通信を行うようにしたので、ＨＴＴＰプロトコルで管理されたネットワーク上でもＩＦＡＸを正常に動作させることができる。

【図面の簡単な説明】

【図１】

本発明の実施の形態１に係る通信制御装置（ＡＤＰＴ）が動作するネットワークを示す概念図

【図２】

実施の形態１に係るＡＤＰＴの動作するグループウェアネットワーク上のクライアント端末周辺における通信プロトコルを説明するための概念図

【図３】

実施の形態１に係るＡＤＰＴのハードウエア構成を示すブロック図

【図４】

実施の形態１に係るＡＤＰＴの主要な機能を示すブロック図

【図５】

実施の形態１に係るＡＤＰＴが接続されたＩＦＡＸからグループウェアサーバに電子メールを送信する場合のシーケンス図

【図６】

実施の形態１に係るＡＤＰＴからグループウェアサーバに電子メールデータを送信する場合のフロー図

【図７】

実施の形態１に係るＡＤＰＴに対してグループウェアサーバから送信される送信フォームデータのソースデータを示す図

【図８】

実施の形態１に係るＡＤＰＴに対してグループウェアサーバから送信される送信フォームの概念図

【図９】

実施の形態１に係るＡＤＰＴが送信する”ＰＯＳＴ”のソースデータを示す図

【図１０】

実施の形態１に係るＡＤＰＴから送信される送信データが記述された送信フォームの概念図

【図１１】

実施の形態１に係るＡＤＰＴが接続されたＩＦＡＸがグループウェアサーバから電子メールを受信する場合のシーケンス図

【図１２】

実施の形態１に係るＡＤＰＴグループウェアサーバから電子メールデータを受信する場合のフロー図

【図１３】

実施の形態１に係るＡＤＰＴに対してグループウェアサーバから送信される受信フォームデータのソースデータを示す図

【図１４】

実施の形態１に係るＡＤＰＴに対してグループウェアサーバから送信される受信フォームの概念図

【図１５】

実施の形態１に係るＡＤＰＴが送信する受信フォームを含む”ＧＥＴ”のソースデータを示す図

【図１６】

実施の形態１に係るＡＤＰＴが出力する受信フォームを含む”ＰＯＳＴ”のソースデータを示す図

【図１７】

本発明の実施の形態２に係るＡＤＰＴのハードウエア構成を示すブロック図

【図１８】

実施の形態２に係るＡＤＰＴの主要な機能を示すブロック図

【図１９】

実施の形態２に係るＡＤＰＴがＩＦＡＸから受信した電子メールデータに対する署名暗号化処理等の処理を示すフロー図

【図２０】

実施の形態２に係るＡＤＰＴがグループウェアサーバから電子メールデータを受信し、その電子メールデータに施された署名暗号化処理等の解読を行うの処理を示すフロー図

【符号の説明】

１００　ＡＤＰＴ

１０１　ＩＦＡＸ

１０３　グループウェアネットワーク

１０４　グループウェアサーバ

２０３　第１ＬＡＮＩ／Ｆ

２０４　第２ＬＡＮＩ／Ｆ

４００　信号種別判定部

４０１　ＳＭＴＰ・ＰＯＰ３処理部

４０２　ＨＴＴＰ処理部

４０３　電子メール通信部

４０４　ＨＴＭＬ通信部

４０５　ＨＴＭＬ処理部

１７０１　ＩＣカード

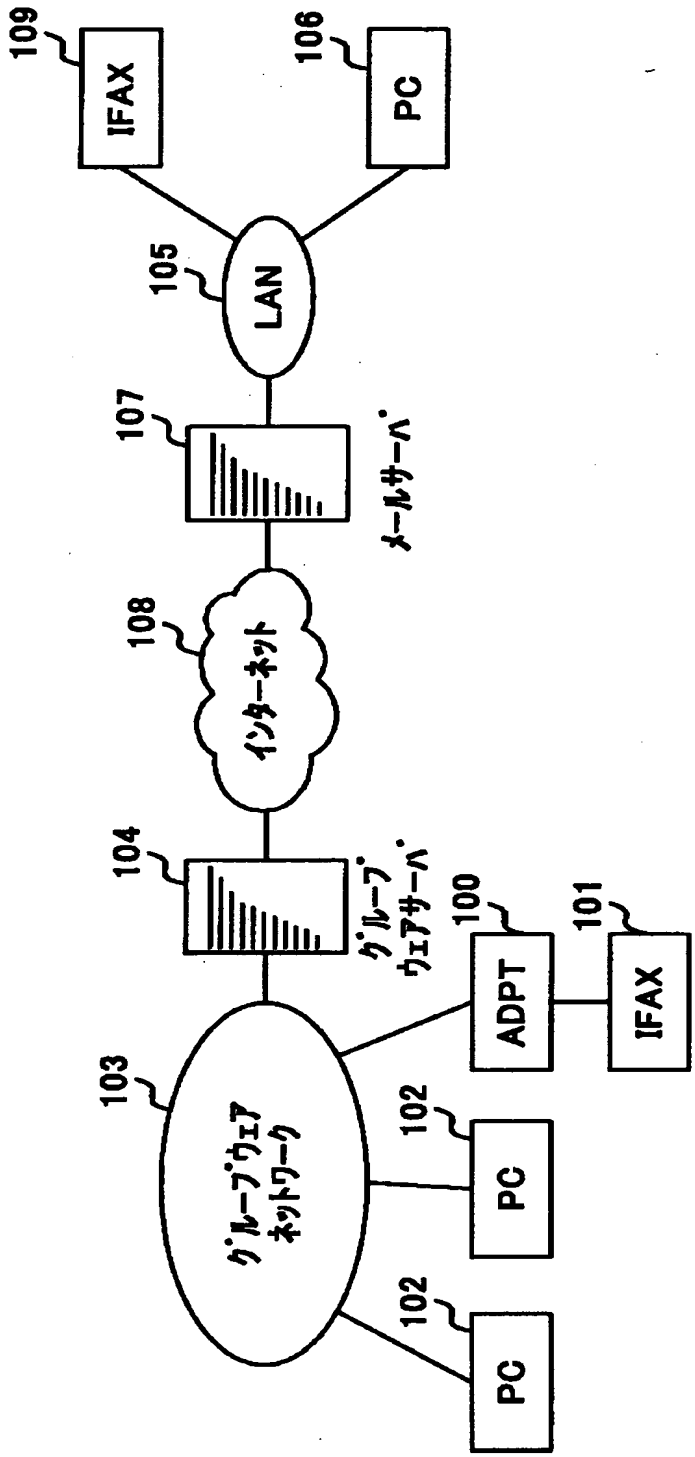
１７０２　ＩＣカードＲ／Ｗ部

１８０１　カード情報判定部

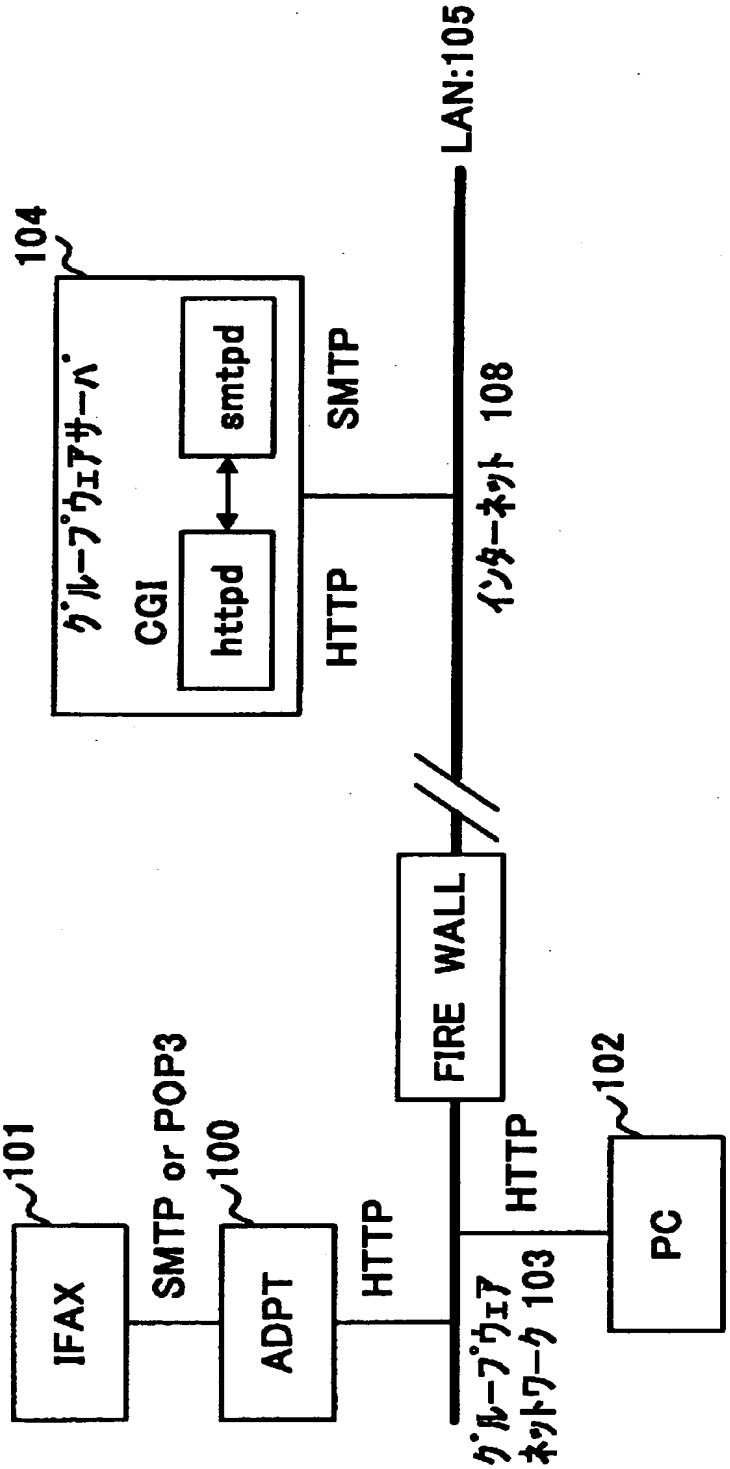
１８０２　署名暗号化処理部

【書類名】　　図面

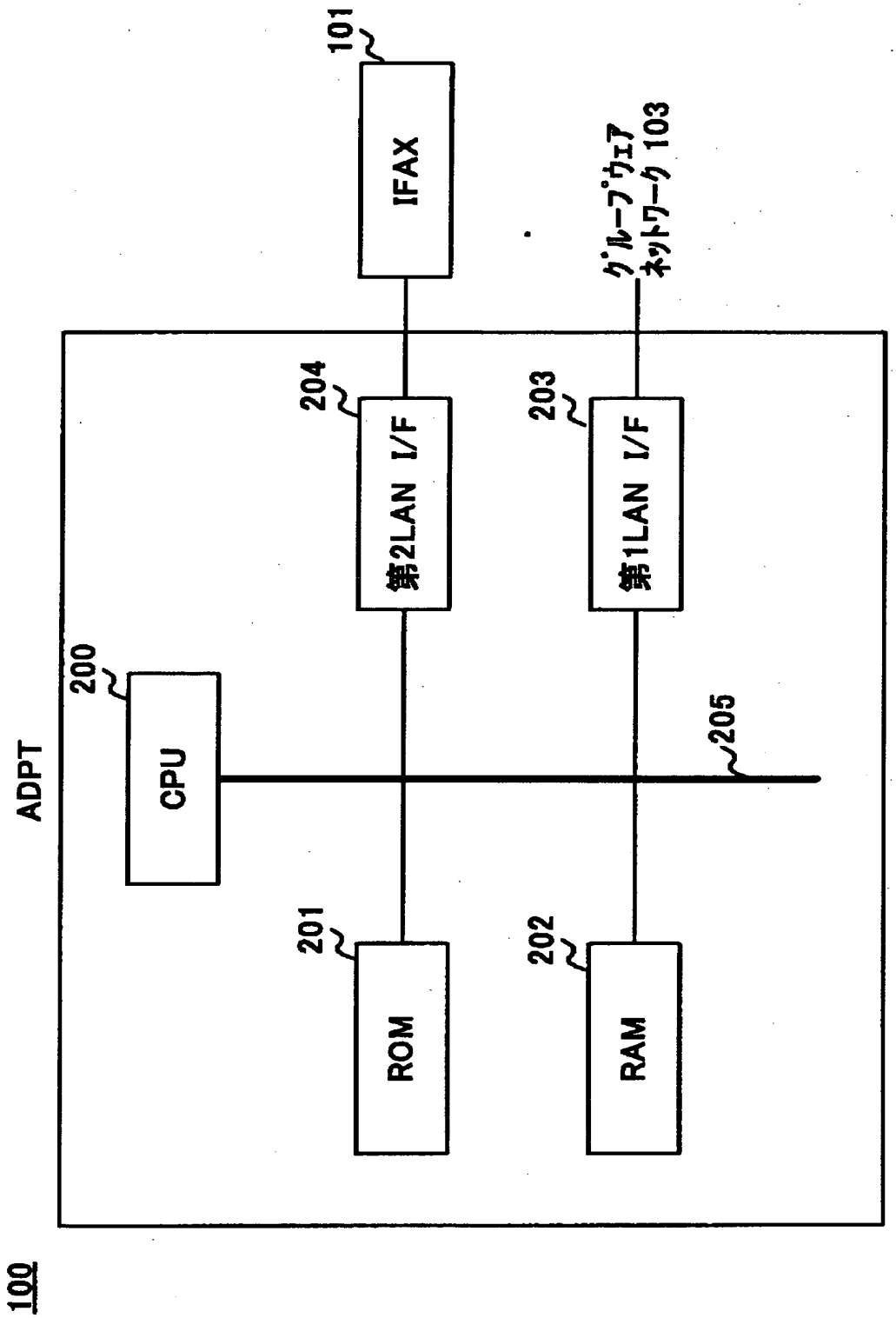
【図１】


109
IFAX
106
PC
105
LAN
107
メールサーバ
108
インターネット
104
グループウェアサーバ
100
ADPT
101
IFAX
103
グループウェア
ネットワーク
102
PC
102
PC

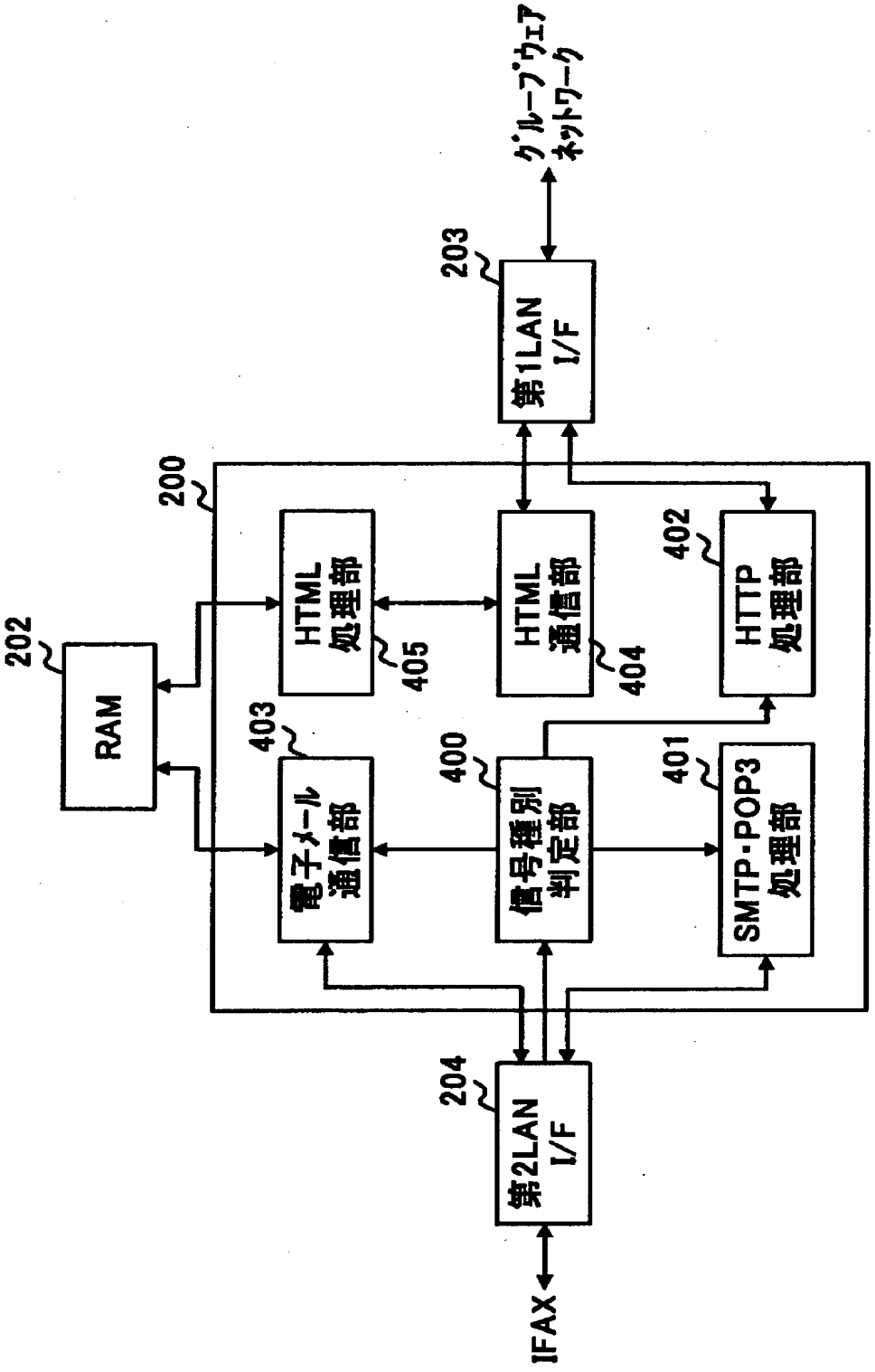
【図２】


LAN:105
104
ｸﾞﾙｰﾌﾟｳｪｱｻｰﾊﾞ
CGI
httpd
smtpd
SMTP
HTTP
ｲﾝﾀｰﾈｯﾄ 108
FIRE WALL
101
IFAX
SMTP or POP3
100
ADPT
HTTP
HTTP
102
PC
ｸﾞﾙｰﾌﾟｳｪｱ
ﾈｯﾄﾜｰｸ 103

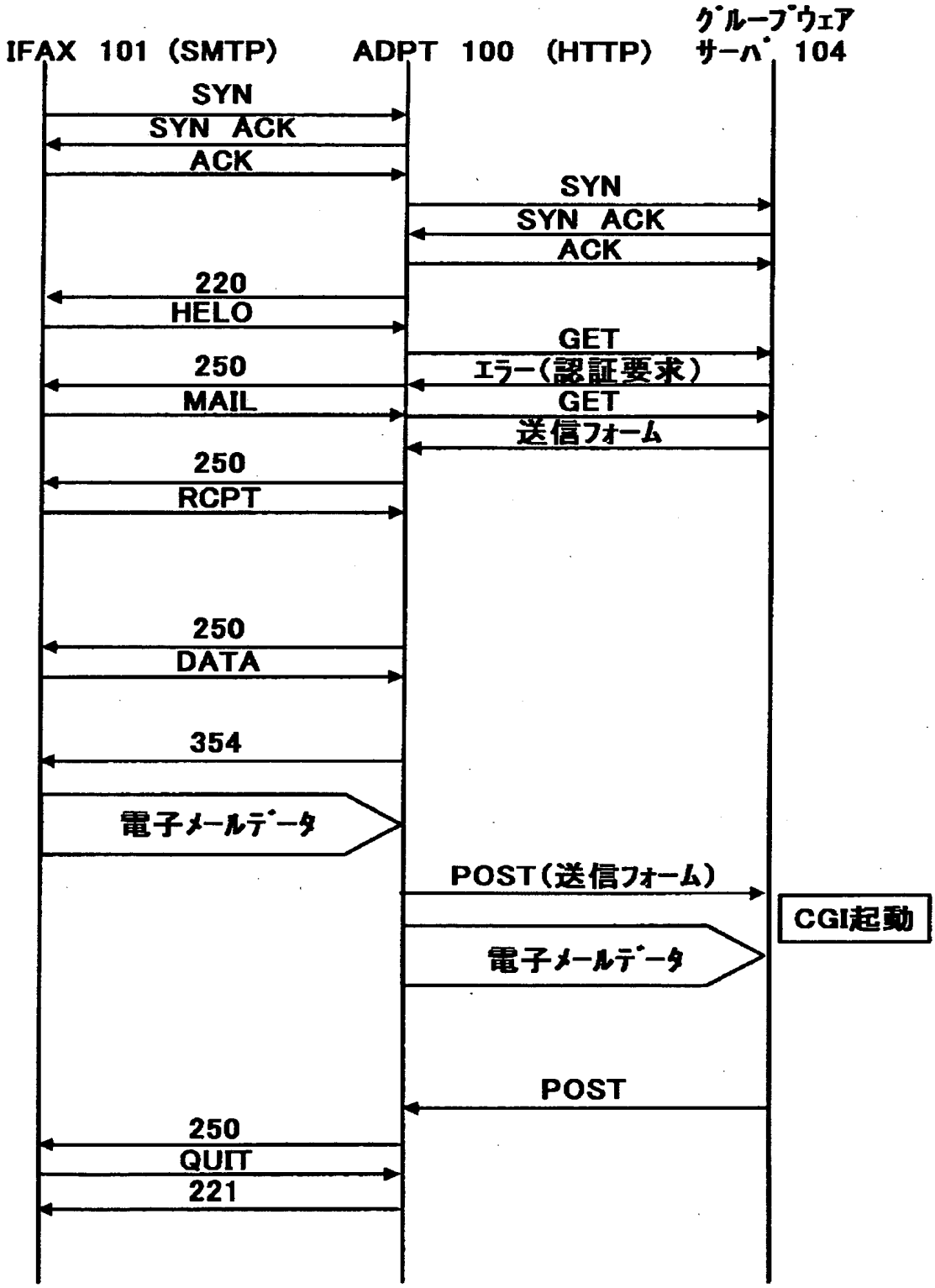
【図３】


101
IFAX
ｸﾞﾙｰﾌﾟｳｪｱ
ﾈｯﾄﾜｰｸ 103
204
第2LAN I/F
203
第1LAN I/F
200
CPU
205
ADPT
201
ROM
202
RAM
100

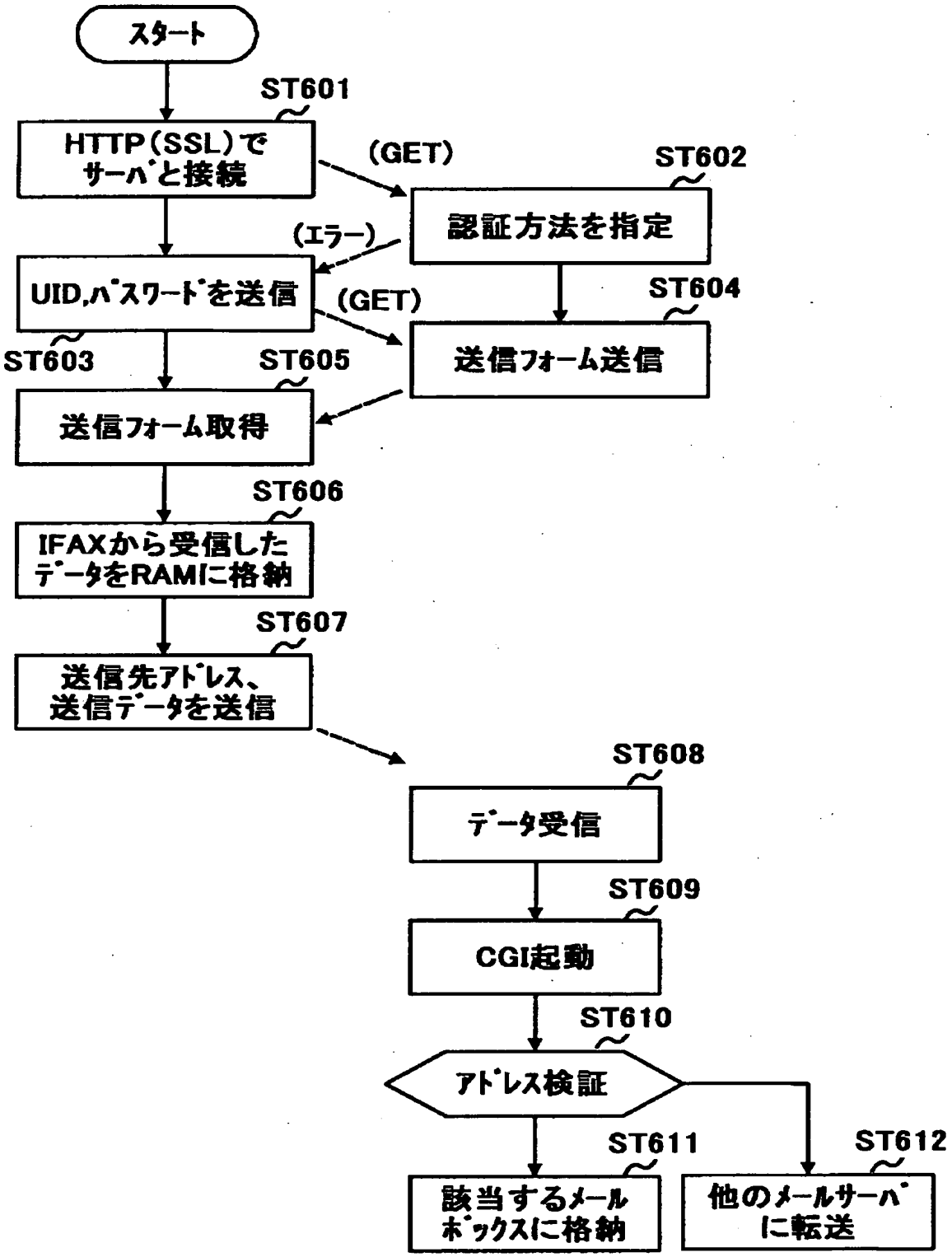
【図４】


グループウェア
ネットワーク
203
第1LAN
I/F
200
HTML
処理部
405
HTML
通信部
404
402
HTTP
処理部
202
RAM
403
電子メール
通信部
400
信号種別
判定部
401
SMTP・POP3
処理部
204
第2LAN
I/F
IFAX

【図５】


IFAX 101 (SMTP)
ADPT 100 (HTTP)
グループウェア
サーバ 104
SYN
SYN ACK
ACK
SYN
SYN ACK
ACK
220
HELO
GET
250
エラー(認証要求)
MAIL
GET
送信フォーム
250
RCPT
250
DATA
354
電子メールデータ
POST(送信フォーム)
CGI起動
電子メールデータ
POST
250
QUIT
221

【図６】


スタート
ST601
HTTP(SSL)で
サーバと接続
(GET)
ST602
認証方法を指定
(エラー)
UID,パスワードを送信
(GET)
ST604
送信フォーム送信
ST603
ST605
送信フォーム取得
ST606
IFAXから受信した
データをRAMに格納
ST607
送信先アドレス、
送信データを送信
ST608
データ受信
ST609
CGI起動
ST610
アドレス検証
ST611
該当するメール
ボックスに格納
ST612
他のメールサーバ
に転送

【図７】

ヘッダ

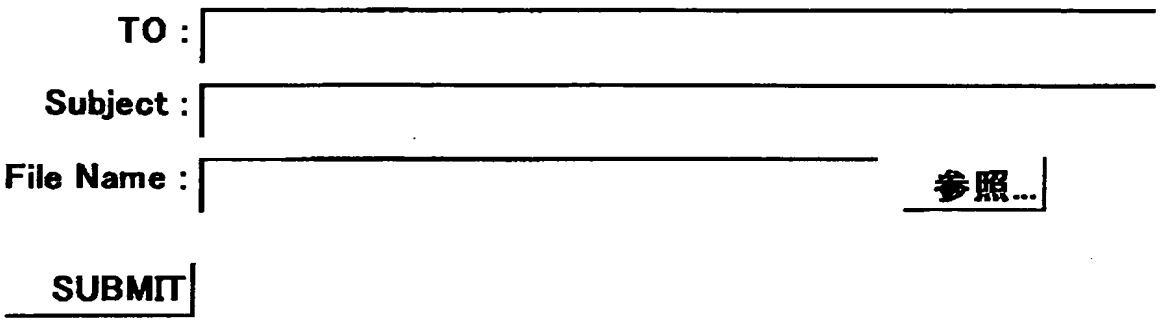
```
HTTP/1.1 200 OK
Date : Fri, 23 Jun 2000 04:13:29 GMT
Server : hoge/1.0
Connection : close
Content-Type : text/html
```

HTML文データ

```
<HTML>
<HEAD><TITLE>TX sample</TITLE>
</HEAD>
<BODY BGCOLOR="#FFFFFFFF">
<FORM ENCTYPE="multipart/fome-data"ACTION="/upload.cgi"METHOD="post">
<TABLE>
<TR><TD ALIGN=right>TO : </TD>
<TD><INPUT TYPE="text"NAME="to"SIZE="60"></TD>
</TD>
<TR><TD ALIGN=right>Subject : </TD>
<TD><INPUT TYPE="text"NAME="subject"SIZE="60"></TD>
</TD>
<TR><TD ALIGN =right>File Name : </TD>
<TD><INPUT TYPE="file"NAME="file"SIZE="45"></TD>
</TR>

</TABLE>
<P><INPUT TYPE=" submit"VALUE="SUBMIT">
</FORM>
</BODY>
</HTML>
```

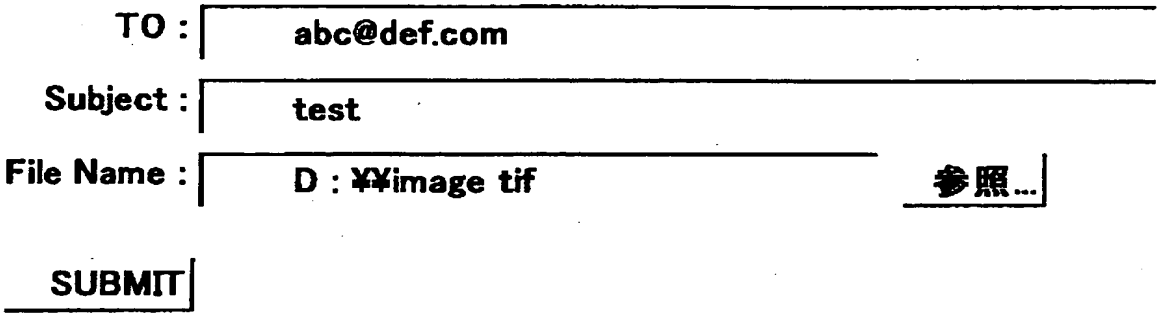
【図８】



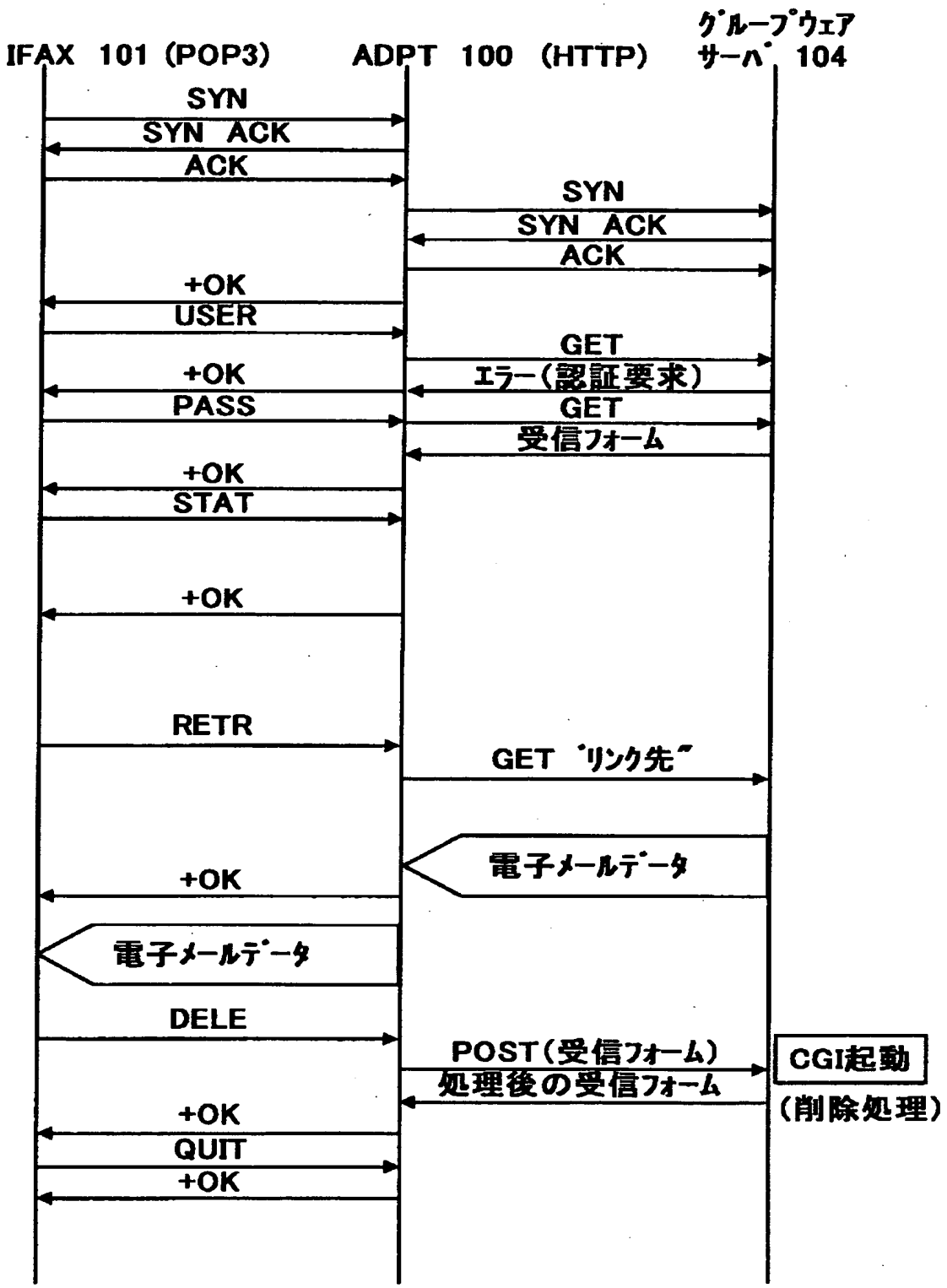
【図９】

ヘッダ
POST/upload.cgi HTTP/1.0
Referer : http ://www.hoge.co.jp/tx.htm
Proxy-Connection : Keep-Alive
User-Agent : foo/1.00
Host : www.hoge.co.jp
Accept : image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Authorization : Basic YXZjYzphdmNj
Content-type : multipart/form-data ; boundary=————————————————81152743116444
送信データ
————————————————81152743116444
Content-Disposition : form-data ; name="to"
送信先
abc@def.com
————————————————81152743116444
Content-Disposition : form-data ; name="subject"
件名
test
————————————————81152743116444
Content-Disposition : form-data ; name="file" ; filename="D : ¥¥image.tif"
ファイル名
II*¥000¥b¥000¥000¥000¥021¥000¥376¥¥¥000¥004¥000
(TIFFデータ)
00¥000¥000¥000¥000¥000¥000¥000¥000¥000¥000¥000¥000¥000¥000¥000
————————————————81152743116444—

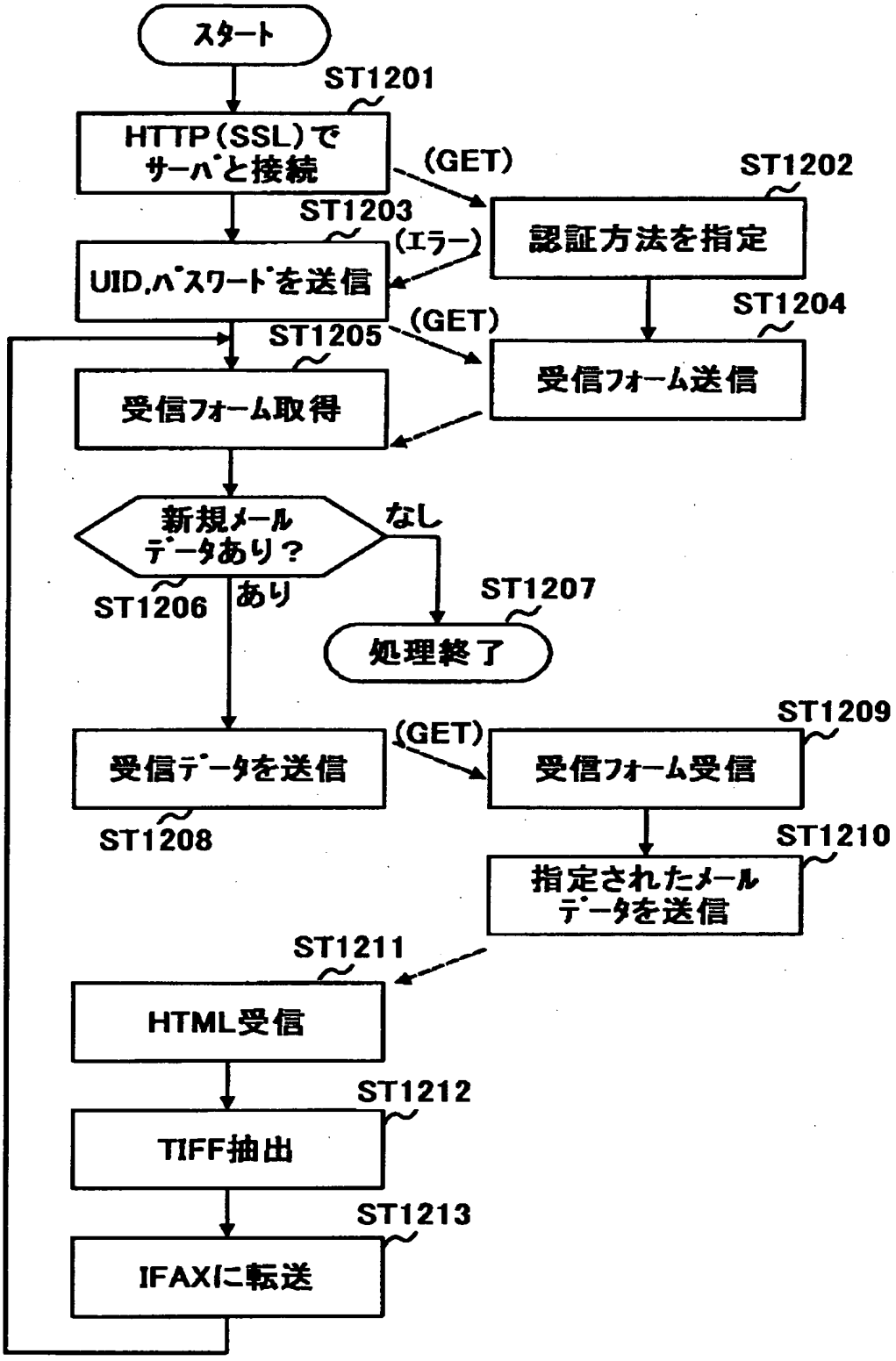
【図１０】



【図１１】


IFAX 101 (POP3)
ADPT 100 (HTTP)
ｸﾞﾙｰﾌﾟｳｪｱ
ｻｰﾊﾞ 104
SYN
SYN ACK
ACK
SYN
SYN ACK
ACK
+OK
USER
GET
+OK
エラー(認証要求)
PASS
GET
受信フォーム
+OK
STAT
+OK
RETR
GET ﾘﾝｸ先
電子メールﾃﾞｰﾀ
+OK
電子メールﾃﾞｰﾀ
DELE
POST(受信フォーム)
CGI起動
処理後の受信フォーム
(削除処理)
+OK
QUIT
+OK

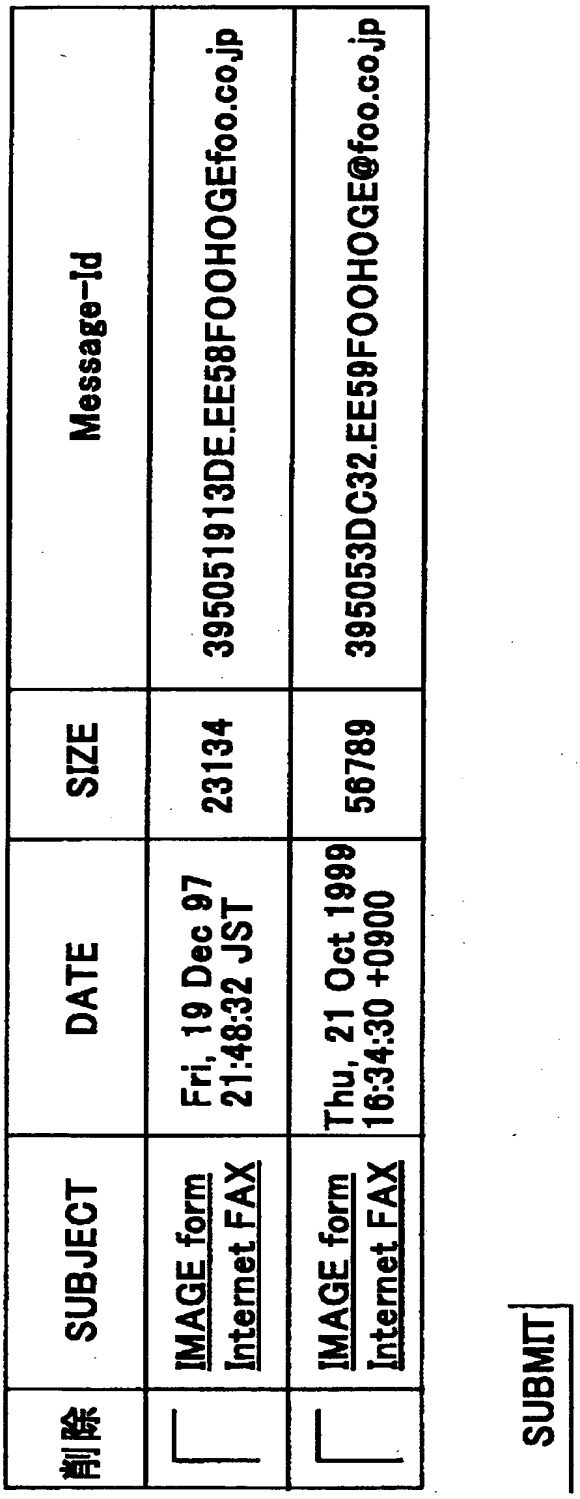
【図１２】


スタート
ST1201
HTTP(SSL)で
サーバと接続
(GET)
ST1202
認証方法を指定
ST1203
(エラー)
UID,パスワードを送信
ST1204
(GET)
ST1205
受信フォーム送信
受信フォーム取得
新規メール
データあり？
なし
ST1206
あり
ST1207
処理終了
ST1209
(GET)
受信データを送信
受信フォーム受信
ST1208
ST1210
指定されたメール
データを送信
ST1211
HTML受信
ST1212
TIFF抽出
ST1213
IFAXに転送

【図１３】

ヘッダ
HTML文データ
HTTP/1.1 200 OK
Date : Mon, 26 Jun 2000 05:06:04 GMT
Server : hoge/1.0
Connection : close
Content-Type : text/html
〈HTML〉
〈HEAD〉〈TITLE〉RX sample〈/TITLE〉
〈/HEAD〉
〈BODY BGCOLOR="#FFFFFFFF"〉
〈FORM ACTION="/download.cgi"METHOD="post"〉
〈TABLE BORDER=1〉
〈TD〉〈TH〉¥215¥355¥217¥234〈/TH〉〈TH〉SUBJECT〈/TH〉〈TH〉DATE〈/TH〉〈TH〉SIZE〈/TH〉
〈TH〉Message-Id〈/TH〉〈/TR〉
〈TR〉〈TD ALIGN=CENTER〉〈INPUT TYPE="checkbox"NAME="D1"〉〈/TD〉
〈TD〉〈A HREF="image000.tif"〉IMAGE from Internet FAX〈/A〉〈/TD〉
〈TD〉Fri, 19 Dec 97 21:48:32 JST〈/TD〉
〈TD〉23134〈/TD〉
〈TD〉395051913DE.EE58FOOHOGE@Foo.co.jp〈/TD〉
〈/TR〉
〈TR〉〈TD ALIGN=CENTER〉〈INPUT TYPE="checkbox"NAME="D2"〉〈/TD〉
〈TD〉〈A HREF="image001.tif"〉IMAGE from Internet FAX〈/A〉〈/TD〉
〈TD〉Thu, 21 Oct 1999 16:34:30 +0900〈/TD〉
〈TD〉56789〈/TD〉
〈TD〉395053DC32.EE59FOOHOGE@foo.co.jp〈/TD〉
〈/TR〉
〈/TABLE〉
〈P〉〈INPUT TYPE="submit"VALUE="SUBMIT"〉
〈/FORM〉
〈/BODY〉
〈/HTML〉

【図１４】


削除
SUBJECT
DATE
SIZE
Message-Id
IMAGE form Internet FAX
Fri, 19 Dec 97 21:48:32 JST
23134
395051913DE.EE58FOOHOGEfoo.co.jp
IMAGE form Internet FAX
Thu, 21 Oct 1999 16:34:30 +0900
56789
395053DC32.EE59FOOHOGE@foo.co.jp
SUBMIT

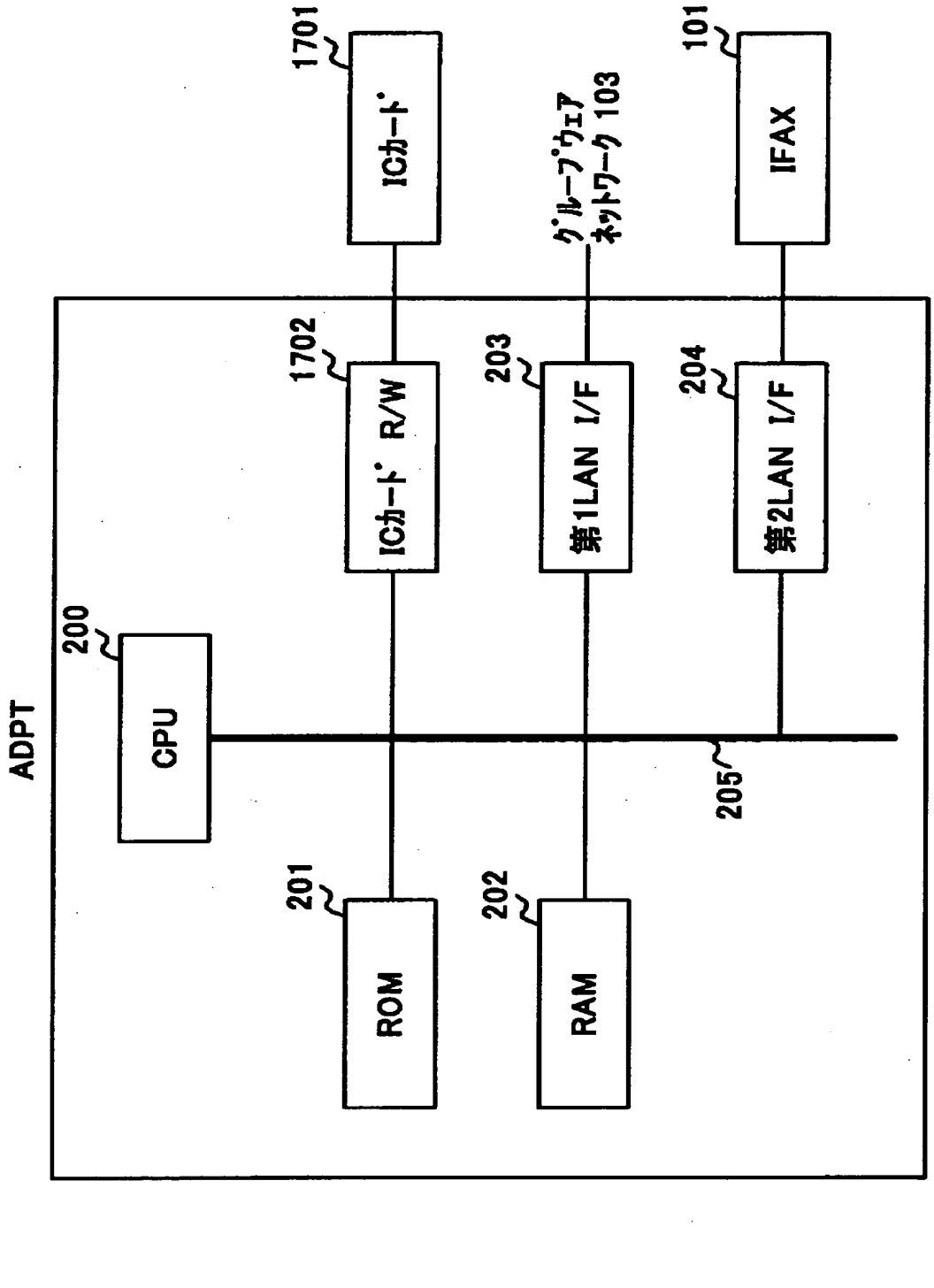
【図１５】

●GETコマンドの例（受信データ要求）
GET/image000.tif HTTP/1.0
Referer : http : //www.hoge.co.jp/rx.htm
Connection : Keep-Alive
User-Agent : foo/1.00
Host : www.hoge.co.jp
Accept : image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Authorization : Basic YXZjYzphdmNj
Cookie : SITESERVER=ID=09d0d169dc148c88b09862f78054e075

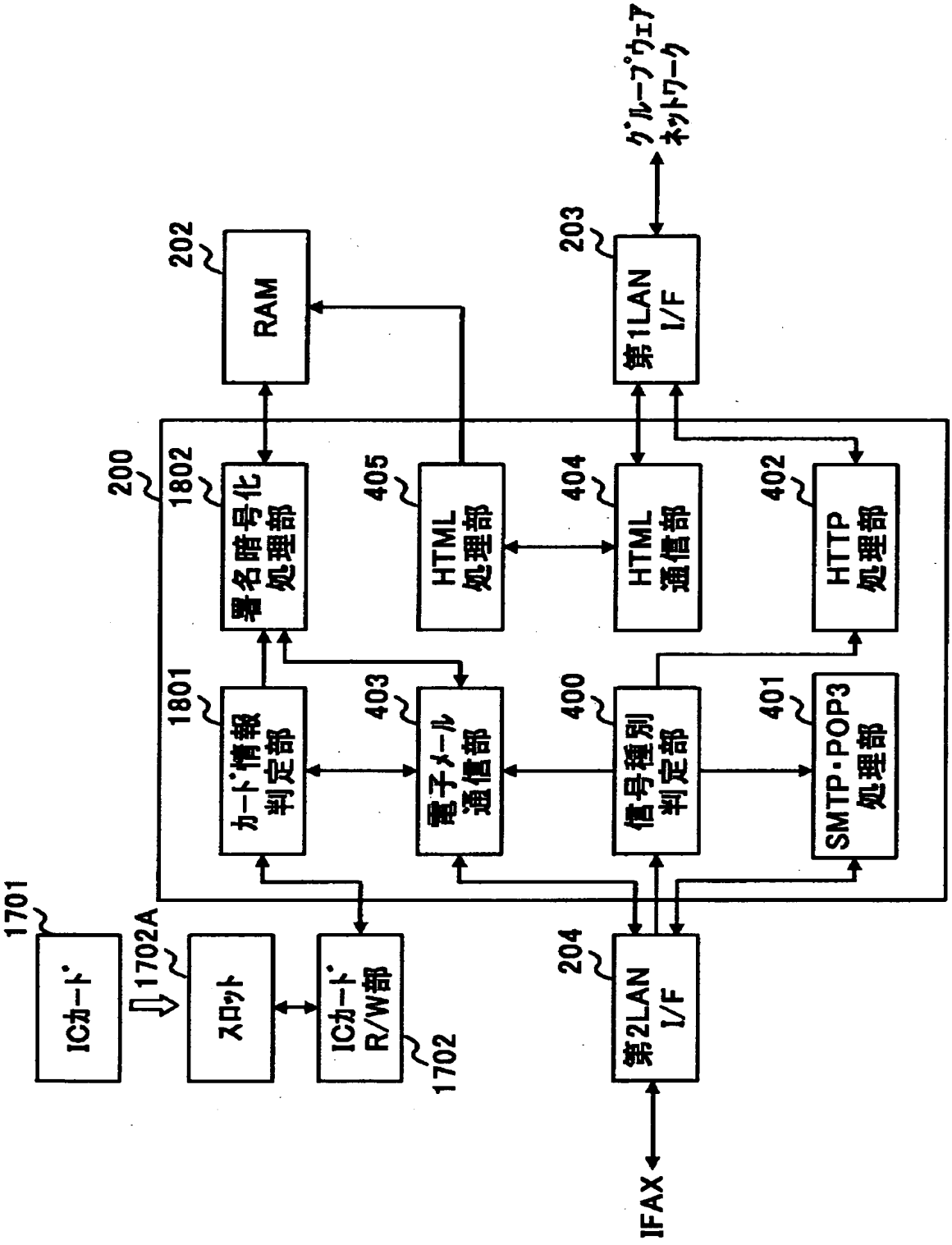
【図１６】

●POSTコマンドの例（削除要求）
POST/download.cgi HTTP/1.0
Referer : http : //www.hoge.co.jp/rx.htm
Connection : Keep-Alive
User-Agent : foo/1.00
Host : www.hoge.co.jp
Accept : image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Authorization : Basic YXZjYzphdmNj
Cookie : SITESERVER=ID=09d0d169dc148c88b09862f78054e075
Content-type : application/x-www-form-urlencoded
Content-length : 5
D1=on
ヘッダ
送信データ

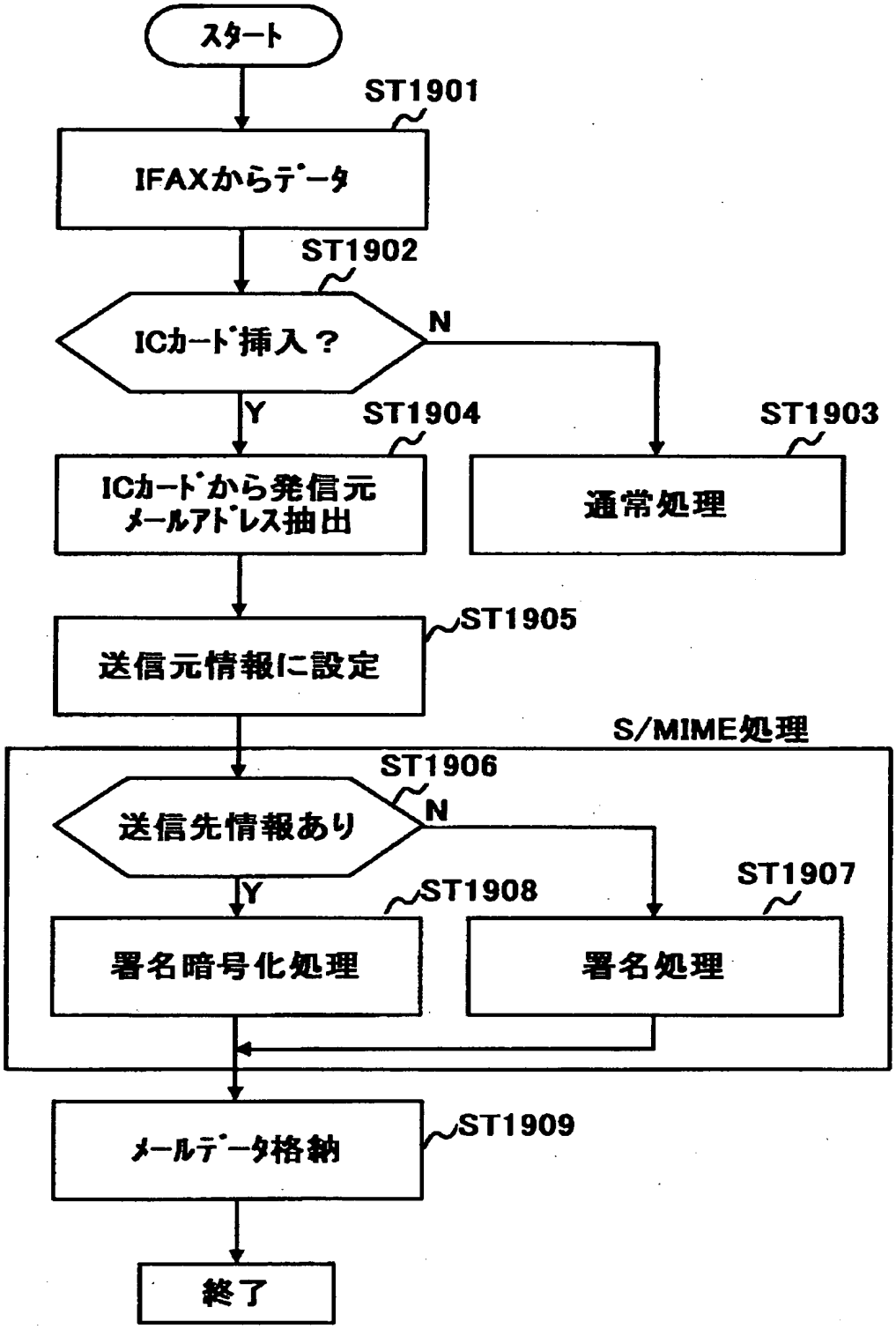
【図１７】


100
ADPT
CPU
200
ROM
201
RAM
202
ICカード R/W
1702
第1LAN I/F
203
第2LAN I/F
204
205
ICカード
1701
グループウェア
ネットワーク 103
IFAX
101

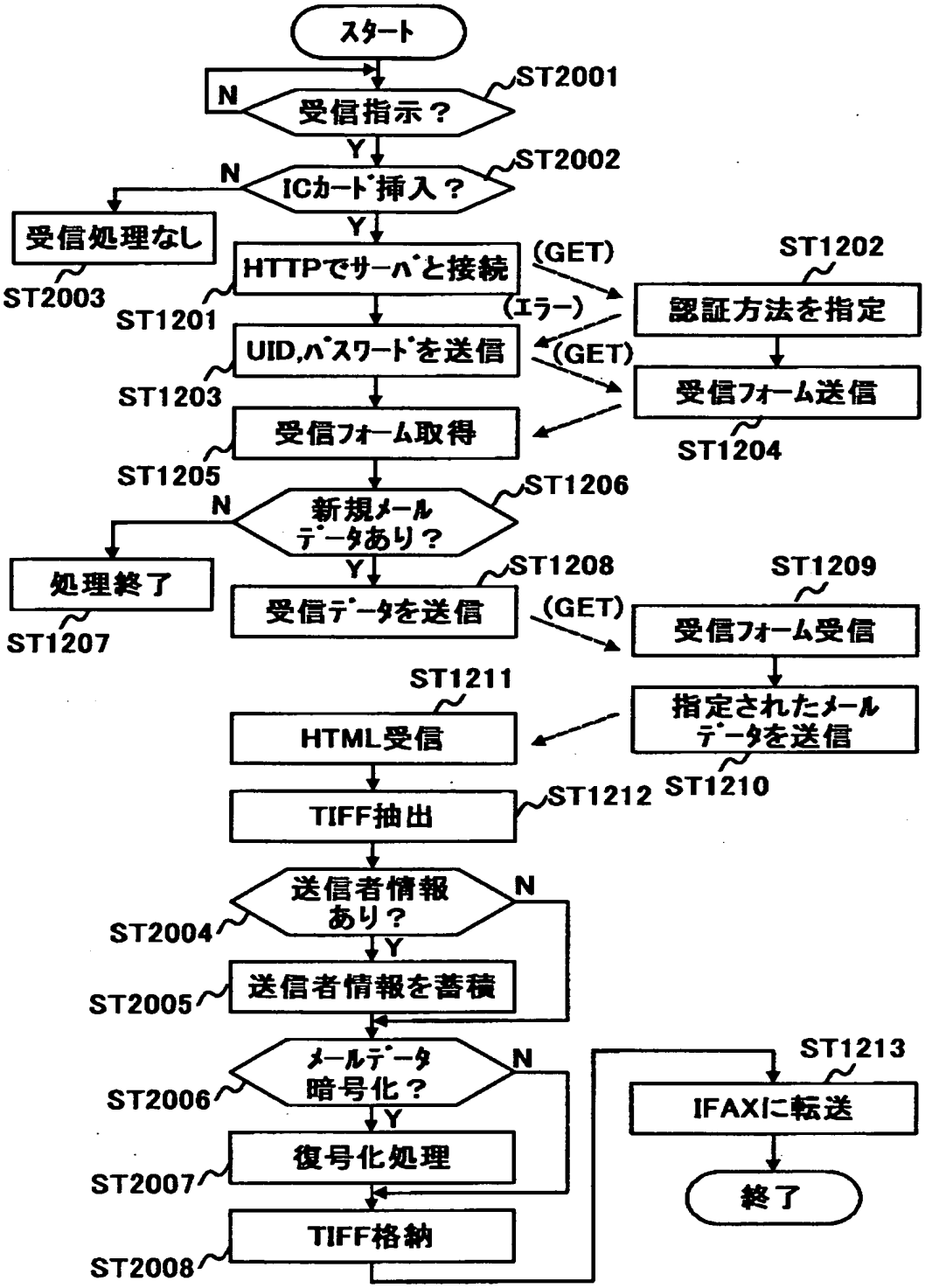
【図１８】


グループウェア
ネットワーク
202
RAM
203
第1LAN I/F
200
1802
署名暗号化 処理部
405
HTML 処理部
404
HTML 通信部
402
HTTP 処理部
1801
カード情報 判定部
403
電子メール 通信部
400
信号種別 判定部
401
SMTP・POP3 処理部
1701
ICカード
1702A
スロット
ICカード R/W部
1702
204
第2LAN I/F
IFAX

【図１９】


スタート
ST1901
IFAXからデータ
ST1902
ICカード挿入？
N
Y
ST1904
ICカードから発信元
メールアドレス抽出
ST1903
通常処理
ST1905
送信元情報に設定
S/MIME処理
ST1906
送信先情報あり
N
Y
ST1908
署名暗号化処理
ST1907
署名処理
ST1909
メールデータ格納
終了

【図２０】


スタート
ST2001
N
受信指示？
Y
ST2002
N
ICカード挿入？
Y
受信処理なし
ST2003
HTTPでサーバと接続
(GET)
ST1202
ST1201
(エラー)
認証方法を指定
UID,パスワードを送信
(GET)
ST1203
受信フォーム送信
受信フォーム取得
ST1204
ST1205
ST1206
N
新規メール
データあり？
Y
ST1208
ST1209
処理終了
受信データを送信
(GET)
受信フォーム受信
ST1207
ST1211
指定されたメール
データを送信
HTML受信
ST1210
TIFF抽出
ST1212
送信者情報
あり？
N
ST2004
Y
送信者情報を蓄積
ST2005
メールデータ
暗号化？
N
ST1213
ST2006
Y
IFAXに転送
復号化処理
ST2007
終了
TIFF格納
ST2008

【書類名】　　要約書

【要約】

【課題】　　ＨＴＴＰプロトコルで管理されたネットワーク上でもＩＦＡＸを正常に動作させること。

【解決手段】　信号種別判定部４００がＩＦＡＸ１０１に接続される第２ＬＡＮインタフェース２０４から送信される、ＳＭＴＰプロトコルに従った所定の信号種別をで判定する。所定の信号種別を判定した場合にＩＦＡＸ１０１との間でＳＭＴＰ・ＰＯＰ３処理部４０１がＳＭＴＰプロトコルに従って通信を制御する一方、ＨＴＴＰ処理部４０２がグループウェアサーバ１０４との間でＨＴＴＰプロトコルに従って通信を制御する。電子メール通信部４０３がＩＦＡＸ１０１から受信した電子メールデータをＨＴＭＬ処理部４０５でＨＴＭＬデータに変換し、ＨＴＭＬ通信部４０４がそのＨＴＭＬデータをグループウェアサーバ１０４に送信する。

【選択図】　　図４

出　願　人　履　歴　情　報

識別番号　　〔０００１８７７３６〕

１．変更年月日　　１９９８年　４月１３日
［変更理由］　名称変更
住　所　　東京都目黒区下目黒２丁目３番８号
氏　名　　松下電送システム株式会社